

RFP 001181Feb 2020

Print Goods and Services UC Systemwide

University of California

Prepared by Scott Reiber
Xerox Technology Advisor

June 5, 2020



June 5, 2020

UC Systems
Michael Wegmann
IT Commodity Manager
Office of the President



Scott Reiber
*Xerox Technology Advisor
Public Sector/Higher Education*
Xerox Corporation
5050 Hopyard Rd. Ste. 100
Pleasanton, CA 94599
scott.reiber2@xerox.com
tel. 925.701.1657

Dear Michael and Committee:

On behalf of the Xerox Team, thank you for the opportunity to present our proposal in response to your RFP 001811 Feb2020 Print Good and Services UC Systemwide.

We have thoroughly reviewed your requirements and are proposing a compliant solution that looks to expand our partnership and will help you achieve your print goods and services goals.

Xerox is a technology leader that innovates the way the world **communicates, connects** and **works**. We understand what's at the heart of sharing information - and all the forms it can take. We embrace the integration of paper and digital, the increasing requirement for mobility, and the need for seamless integration between the employee's work and personal worlds. We also recognize the need for security compliance, sustainability and how to work in the new world of today.

Innovation and continuous improvement are key pillars of our Execution Methodology. Our philosophy is "Customers for Life", which embodies the importance we place in our partnerships and delivering ongoing excellence to customers like University of California.

Thank you for your consideration and confidence in Xerox. We look forward to the next steps you're your procurement process and continuing as your trusted partner for print goods and services.

Regards,

Scott A Reiber

Scott Reiber
Technology Advisor

Table of Contents

Table of Contents	3
Xerox Clarifications/Exceptions to the Regents of the University of California RFP Print, Goods and Service	4
Xerox's Clarifications to the University's RFP	4
Attachments	14

Xerox Clarifications/Exceptions to the Regents of the University of California RFP Print, Goods and Service

We have reviewed the University's Request for Proposal ("RFP") and have prepared the enclosed Purchase and Maintenance and 36, 48 and 60-months Lease Proposal (Fair Market Value, \$1 Buyout Option) subject to the University's contract standards or performance for your consideration. In addition, Xerox has also included a separate pricing and Terms & Conditions response for Non-University members subject to Omnia Partners contract standards of performance and terms and conditions. All operational requirements for the University in the contract, such as customized reporting and separately billed maintenance are applicable for University only. All operational requirements, performance standards and terms and conditions of the master agreement Xerox/Omnia contract are applicable for non-University customers. Although the Proposal is based on the requirements included in your RFP, our Proposal does include some responses that are slightly different. This document and our Proposal explain those differences. In addition, we have included some Additional Terms that were not addressed in the University's RFP. Please note that Xerox's Proposal is contingent upon the accuracy of the information included in the University's RFP and Xerox's review of the University's credit. Any material change to the information provided by the University, or the University's credit, may result in a change to Xerox's offer.

Please note that Xerox agrees to negotiate a solution that is acceptable to both parties if any of the below clarifications or Additional Terms are inconsistent with California law, or are otherwise unacceptable to the University. Our team is also prepared to discuss our Proposal in detail, and adjust our proposed equipment, support services, terms, and/or price offering based on the University's final requirements. Upon award of this RFP, Xerox agrees to negotiate a Contract that incorporates the mutually agreed terms contained in the University's RFP, our Proposal, Xerox's Purchase and Maintenance and Lease Agreement (applicable to the University and its affiliates), and OMNIA Partner's terms and conditions (applicable for Non-University members), and any additional negotiated item(s).

Xerox's Clarifications to the University's RFP

Xerox provides the following clarifications and comments to the below listed University RFP requirements.

RFP EVENT AND PROCESS SUMMARY

SECTION 3. MFD/PRINTER FLEET MANAGEMENT PROGRAMS; 3.1.1.1 MFD 36//48/60-months terms.

The Xerox Lease offering is based on a firm 36-month, 48-month and 60-month, FMV and \$1 Buy-out Option, of equipment installation commitment, and consists of a Monthly Base Charge that covers the cost of the equipment; the cost per copy and overage rates, any trade-in equipment refinanced / buyout amounts; an equipment trade-in credit value; the equipment's FOB shipment, freight, and inside delivery and removal (excluding any unique rigging expenses); the equipment's physical installation and connection to the University's network; and end user initial training, and the labor services detailed in our Proposal. Remote installations are also available where applicable.

Please note Xerox does not offer any trade bonuses for sale to lease equipment transactions under this Agreement. For competitive sale to sale trades Xerox will remove the competitive/owned equipment at Xerox expense.

SECTION 3. MFD/PRINTER FLEET MANAGEMENT PROGRAMS; 3.1.1.2 and 3.1.1.3 Discounts.

Outright Purchase Equipment. Please note Xerox will provide an additional 5% discount on the published University equipment mainframe price (excluding accessories) list for Outright Sale/FMV & FPO Lease (equipment price only, excluding maintenance) for orders for Managed Programs. Any/all discounts will be taken at the time of order.

Lease Equipment. Please note Xerox cannot guarantee any additional discounts beyond the published lease price however, Xerox will review/consider these opportunities for additional discounts for "Managed Programs" upon request.

SECTION 4. PRODUCT CERTIFICATION

Equipment provided under the Contract is currently manufactured by Xerox, though the equipment may contain recycled components that have been reprocessed to meet Xerox' new parts performance standards. The County will be the first user of the equipment.

SECTION 5. PROGRAM FOR TRADE-INS/UPGRADES

Trade-In Equipment. Xerox warrants that University has the right to transfer title to the Equipment University is trading in as part of an Order ("Trade-In Equipment"), and that the Trade-In Equipment is in good working order and has not been modified from its original configuration (other than by Xerox). Title and risk of loss to the Trade-In Equipment will pass to Xerox when Xerox removes the Trade-In Equipment from University premises. University will maintain the Trade-In Equipment at its present site and in substantially the Trade-In Equipment's present condition until removed by Xerox. University will pay all accrued charges for the Trade-In Equipment, up to and including payment of the final principal payment number and all applicable maintenance, administrative, supply and finance charges until Xerox removes the Trade-In Equipment from the University's premises.

Upgrades. Xerox's Purchase and Maintenance as well as Xerox Lease offer allows the University to place additional equipment mainframe orders at the same quoted contract price throughout the 60-month master agreement term, provided each additional equipment placement remains installed for a minimum 36/48/60-month term. Xerox will also provide a separate price quote if the University desires to acquire additional equipment having an installation term less than 60-months. The equipment's features and performance can also be upgraded through the addition of a number of optional accessories. Accessory options included with the mainframe can be obtained at the contract quoted price. Any accessory ordered following the mainframe's installation will have the price readjusted based on the mainframe's remaining agreement term.

Please remember that the Xerox Purchase and Maintenance as well as Xerox Lease offering is based on a firm 36/48/60-month equipment installation term that can only be terminated due to fiscal year funds non-appropriation or an uncured performance failure. If the equipment is cancelled for the University's convenience and not replaced, or traded to a different unit, the University will be assessed a liquidated damages charge. In order to avoid this charge, Xerox recommends that the equipment either be: (a) exchanged with another University unit, or (b) moved to another University location and replaced with a unit that fits the end users current work requirements.

D. Organizational Context.

University of California Pricing Terms - For University of California and affiliates Xerox agrees to extend the specific University product pricing and terms of this Agreement.

OMNIA Partners' National Master Agreement– Xerox agrees to make resulting OMNIA Partners' pricing/terms from this solicitation available to other public agencies nationally, including state and local governmental entities, public and private primary, secondary and higher education entities, non-profit entities, and agencies for the public benefit ("Public Agencies") through OMNIA Partners' Cooperative purchasing program so long as such Public Agency is a registered member at OMNIA. Non-University OMNIA members will procure equipment and services subject to the terms and conditions of the OMNIA Master Agreement which terms are hereby incorporated by their reference <https://www.sourcewell-mn.gov/cooperative-purchasing/083116-xox?domain=870%20%20%20%20%20%20%20%20%D0%B5H#tab-contract-documents>

3 MFD/Printer Fleet Management Programs - Delivery and Installation.

Delivery. Please note the following will apply to any Purchase and Lease transaction: Unless otherwise agreed upon by the parties, Xerox equipment deliveries can normally be expected within ten business days following the receipt of the University's equipment approved and accepted purchase order, except during times of product constraint. Xerox will inform the University if a constraint condition exists and will provide a revised delivery date. If the revised target delivery date is unacceptable, the University can cancel the order without penalty to either party.

Installation. Unless the Purchase and Maintenance and Lease Agreement is preceded by a Trial order, the equipment will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

2.2 Equipment Service and Support

Uptime. Total Uptime Xerox's Uptime objective is to maintain an average 96% equipment uptime performance based on a three-month rolling average for the University's entire Xerox-branded equipment population that is operated with the equipment's operating guideline for the specified product. Uptime is calculated as follows:

- 1. UPTIME TARGET.** Provided Customer has at least twenty-five (25) units of Equipment installed under this Agreement, Xerox agrees to maintain an Uptime Target for the total Equipment population installed under this Agreement, which shall be measured as provided below over a three (3) calendar month rolling period, of at least ninety-six percent (96%) in the aggregate for the Equipment subject to this Agreement that is operated within the specified Maximum Monthly Volume Range, (to be included upon University's request in an Appendix to this Contract) and installed within twenty-five (25) miles of a Xerox service location. This Uptime Target commences on the first day of the calendar month that begins at least one hundred twenty (120) days after the Agreement commences.
- 2. CONTRACTED PERIOD OF COVERAGE.** Xerox will provide Maintenance Services, as the same is set forth in this Agreement, during Customer's normal business hours Contracted Period of Coverage ("CPOC"), which shall be defined as 9:00 a.m. to 5:00 p.m., Local Time, Mondays through Fridays (excluding Xerox-recognized holidays), for the purposes of this Agreement.
- 3. UPTIME HOURS DEFINITION.** "Uptime Hours" equals the number of hours per calendar month that the Equipment is available for use. For this Agreement, Uptime Hours equals 567 hours per three (3) calendar months and has been calculated by multiplying the number of hours per day in the CPOC times the average number of days per three (3) calendar month period such coverage is provided, which, for the purposes of this Agreement, is sixty-three (63) days per three (3) calendar month period..

4. **DOWNTIME HOURS DEFINITION.** "Downtime Hours" shall mean the number of hours in any three (3) calendar month period during which Equipment maintained hereunder is inoperative (i.e., cannot make any copies or prints, as applicable) during the CPOC, including machine-repair time and response time when the Equipment is inoperative. Downtime Hours do not include time when the Equipment's inoperability is due to user misuse or abuse of the Equipment, Customer's negligence or intentional acts, fire, environmental failure at the installation site or use of the Equipment in a manner other than was intended; preventative maintenance, Equipment relocation or inspections are being performed; and, time taken in producing usable copies or prints.

5. **CALCULATION.** The Uptime Percentage Rate for a given calendar month is calculated as follows:

$$\text{Uptime Percentage Rate} = \frac{\text{CPOC (567)} - \text{Downtime Hours (x)}}{\text{CPOC Hours (567)}}$$

Laser Printers.

Lease: For FMV/FPO leases the Maintenance is included and begins upon install.

Response/Repair Time. Xerox's response time objective is to return all service calls within one business hour, and to arrive on-site on average within 3.5 to 4 business hours for multifunction color devices, if the problem cannot be resolved over the phone. Response Time for other devices will be provided upon request. Response time is calculated based on the quarterly response time average for the University's entire Xerox-branded equipment population. Calls can be placed toll free 24-business hours per day, 7 days per week, and 365 days a year. During standard business hours (8 A.M. to 5 P.M., Monday thru Friday), all service calls will be directed to our Service Welcome Center where our service personnel will attempt to resolve the issue over the phone through on-line diagnostics. If the problem cannot be resolved over the phone the representative will provide the caller with the technicians estimated time of arrival. The Service Technician will contact the caller prior to arriving on-site to discuss the problem and determine if they have the appropriate parts, or if there will be a change to the arrival time. Evening, weekend, and holiday phone service is also available. On-site evening, weekend, and holiday service support can also be prearranged or may be available based on evening resource availability. The 24x7-call center and business hour technical support is included in our contract offering. After hour, weekend, and holiday on-site technical support is available at Xerox's then current overtime rate. Please refer to the XPS Description of Services for response time objectives relating to the XPS / Managed Print Services offering.

Delivery/Installation.

Delivery. Please note the following will apply to any Purchase and Lease transaction: Unless otherwise agreed upon by the parties, Xerox equipment deliveries can normally be expected within ten business days following the receipt of the University's equipment approved purchase order, except during times of product constraint. Xerox will inform the University if a constraint condition exists and will provide a revised delivery date. If the revised target delivery date is unacceptable, the University can cancel the order without penalty to either party.

Installation. Unless the Purchase and Maintenance and Lease Agreement is preceded by a Trial order, the equipment will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

Attachment – University Terms and Conditions of Purchase

Article 2. Term and Termination.

Xerox recognizes the University's right to terminate the Agreement for its convenience due to a change in its business needs. However, the Xerox offer is based on a firm 36, 48, or 60-month equipment installation commitment, and cannot be terminated except for fiscal year funds non-appropriation or uncured Xerox default.

In order to terminate the Agreement due to non-appropriation, University must provide Supplier with written notice, within 31-days of its governing body's decision not to appropriate funds, stating that the University's governing body failed to appropriate funds. The notice must certify that the canceled equipment is not being replaced by equipment performing similar functions during the ensuing fiscal year. In addition, the University will be required to return the equipment to Supplier with transportation costs borne by Supplier. The University will then be released from its obligation to make any further payments beyond those through the end of the last fiscal year for which funds have been appropriated.

University may terminate this Agreement for convenience at any time, in whole or in part, in accordance with the terms of Article 2 of University of California Terms and Conditions of Purchase. In the event of such termination, University agrees to provide Xerox at least thirty (30) days prior written notice of the effective date of termination and the extent thereof, such termination shall not affect any leased unit that has not fulfilled the appropriate term.

If any termination of this Agreement takes place, Xerox shall extend to University, upon University request, an additional ninety (90) day period to properly implement a smooth transition. Fees for the services performed during the additional ninety (90) days will be in good faith negotiated between University and Xerox. Termination under this provision, shall not apply to orders received by Xerox prior to the effective date of termination.

In the event Xerox cannot or does not perform its obligations, University reserves the right to terminate the Agreement. If within thirty (30) days of receipt of written notice from University of Xerox's breach of any term or condition of the Agreement, Xerox shall fail to remedy such breach, then University may terminate the Agreement. However, this cancellation provision does not pertain to any leased equipment installed prior to University's termination notice. In the event the Agreement is terminated, individual lease placements will continue until their scheduled expiration date, and continue to be governed by, and be subject to, the terms and conditions of the individual lease and the Agreement.

Article 3. Pricing, Invoicing Method, and Settlement Method and Terms. Xerox will not issue an invoice until Services have been rendered and accepted. University will pay Xerox, within thirty-one (31) days of receipt of an undisputed and accurate invoice. The agreed upon minimum lease payment will not be subject to dispute at any time. Xerox will not issue an invoice until Services have been rendered and accepted.

Article 4. Inspection. Xerox can support the University's inspection and acceptance requirement by initially installing the equipment under a Trial arrangement. Unless an order is preceded by a Trial order, the Services will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

Article 6.j Outsourcing (Public Contract Code Section 12147 Compliance). All services included in the Xerox bid to be specifically contracted for by the University will be provided within the U.S. However, certain back-office contract administration and customer support services are performed by Xerox and/or its affiliates from locations outside the U.S.

Article 7. Intellectual Property. Xerox does not anticipate the development of any customized products or programming in connection with the services provided under the Contract. Xerox agrees that all University authored documents printed/copied on Xerox supplied equipment is the University's sole and exclusive property, and that Xerox shall have no rights to these documents. Also, all Xerox generated reports and the output of Services is Customer's sole and exclusive property and Xerox will have no rights to these documents or data, except as may be required for Xerox to perform Services. All other work prepared by or processes developed by Xerox for the University's use will remain the sole property of Xerox and is not deemed a "work for hire". However, Xerox grants the University a non-exclusive, perpetual, fully paid-up, world wide right to use, display, reproduce, and modify any report, form, design, computer programs, code, or other work of authorship provided by Xerox to the University in the course of performing the Services under the Contract strictly for the University's internal business use and not for resale or distribution outside of the University's organization.

Article 8. Indemnity and Liability.

Indemnification is contingent upon University giving Xerox written notice, by registered mail, promptly after it becomes aware of any claim to be indemnified hereunder and permits Xerox to control the defense of any such claim or action and Xerox's own expense. Notice shall be sent to "Corporate Risk, Xerox Corporation, Long Ridge Road, Stamford, Connecticut, 06940." University agrees that Xerox may employ attorneys of its own choice to appear and defend the claim or action and that University shall do nothing to compromise the defense of such claim or action or any settlement thereof and shall provide Xerox with all reasonable assistance which Xerox may require. Xerox shall not be obligated to indemnify the University against the University's own acts or omissions.

Except for indemnified matters and to the extent permitted by applicable law, all other liability of Xerox to University for damages of any kind of type, including but not limited to indirect, consequential, incidental, or special damages, arising from Xerox performance or failure to perform under this Contract or by virtue of Xerox's tortuous conduct (including negligence whether passive or active) shall be limited to the amounts paid by University under this Agreement. Provided, however, that the foregoing limitation of liability shall not apply to claims by University for personal injury or damage to real or tangible property caused by Xerox's negligence.

Article 9. Insurance. Xerox agrees to include the University as an additional insured under the comprehensive general liability and automobile liability insurance policies only for claims arising out of the willful or negligent acts, or omissions of Xerox in the performance of the services under the contract. Xerox and University will agree on the final coverage required under this Proposal.

Article 17. Additional Terms Applicable to the Furnishing of Goods

A. Price Decreases.

Xerox agrees immediately to notify the University of any price decreases from its suppliers, and to pass through to UC any price decreases. Any price reduction resulting from this provision shall only apply to orders received after the effective date of the price reduction.

B. Title. Title to the Goods purchased under the Agreement, along with the risk of equipment's loss or damage, will pass directly from Xerox to University upon delivery, subject to University's right to reject upon inspection.

Article 20. Prohibition on Unauthorized Use or Disclosure of Institutional Information; (e) No Offshoring.

All services included in the Xerox bid to be specifically contracted for by the University will be provided within the U.S. However, certain back-office contract administration and customer support services are performed by Xerox and/or its affiliates from locations outside the U.S.

Article 27. Force Majeure. This provision does not relieve either party of its obligation to make payments due under the Contract. Any University purchases to procure the services from other sources without Xerox's prior approval will be at the University's expense.

Attachment – University Terms and Conditions of Equipment Lease

Article 2. Inspection. Xerox can support the University's inspection and acceptance requirement by initially installing the equipment under a Trial arrangement. Unless an order is preceded by a Trial order, the Services will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

Article 5. Termination. Xerox recognizes the University's right to terminate the Agreement for its convenience due to a change in its business needs. However, the Xerox offer is based on a firm 36, 48, or 60-month equipment installation commitment, and cannot be terminated except for fiscal year funds non-appropriation or uncured Xerox default.

The initial term for any individual lease order will be the number of full calendar months stated in the order. The minimum lease payment for any partial month following the equipment installation date will be billed on a pro rata basis, based on a 31-day month. The term for each unit of equipment will commence upon the delivery of customer-installable equipment; or the installation of Xerox-installable equipment and will expire on the last day of the final full calendar month of the contracted term indicated in the order.

University may at its option, by written notice stating the extent and effective date, terminate this order at the anniversary date of the lease or at the end of any fiscal year in whole or in part in the event the funding agency does not appropriate sufficient funds to continue the lease payments.

In order to terminate the Agreement due to funding non-appropriation, the University must provide Xerox with written notice, within 30-days of its governing body's decision not to appropriate funds, stating that the University's governing body failed to appropriate funds. In addition, the University will be required to return the equipment to Xerox with transportation costs borne by Xerox. The University will then be released from its obligation to make any further payments beyond those through the end of the last fiscal year for which funds have been appropriated. Other than as stated above, leases may not be cancelled prior to expiration. Early cancellation of individual leases without cause or cancellation of individual leases by Xerox due to the University's material breach will result in an early termination charge that is equal to the sum of the remaining payments less any unearned maintenance and supply charges discounted at 4% per annum. In no event shall the amount paid exceed the total contracted price, minus payments already made.

Xerox will provide University with no less than thirty-one (31) days advance notice of the expiration of each lease term. Upon lease expiration, University shall have the option to:

- Purchase the equipment AS IS, WHERE IS, by giving Xerox at least thirty (30) days prior notice of University intent to purchase at the termination of the term specified in any order or any renewal thereof. The purchase

option price for FMV leases shall be the equipment's then fair market value plus all applicable sales taxes. The purchase option for FPO will be \$1 plus all applicable sales taxes.

- Lease the current equipment at the same monthly price on a month-to-month basis. This type of lease extension may be cancelled without penalty upon 30 days written notice.
- Have Xerox provide a quote on a new 12- or 24-month lease on the current equipment. This will yield a lower monthly price; however, the University would not be able to cancel the lease without termination charges until expiration of the new extended lease.

Upon expiration of a lease without extension, University will make the equipment available for removal by Xerox at Xerox's cost. At the time of removal, the equipment will be in the same condition as when delivered, reasonable wear and tear accepted.

A lease order under the contract is a "finance lease" under Article 2A of the Uniform Commercial Code and, except to the extent expressly provided under the Contract, and to the extent permitted by California law, Customer waives all rights and remedies conferred upon a lessee by Article 2A.

Article 6. Title. Title to the Goods purchased under the Agreement, along with the risk of equipment's loss or damage, will pass directly from Xerox to University upon delivery, subject to University's right to reject upon inspection.

Article 11. Proprietary Rights Indemnity. Xerox will agree to this indemnity provision providing Xerox is given written notice of the claim or action and allowed to select attorneys of its own choice to appear and defend the claim or action. In addition, the University agrees to provide Xerox with all reasonable assistance that Xerox may require, and that the University will do nothing to compromise Xerox's defense or settlement of the claim or action. Xerox agrees that it will be responsible for its equitable share of any claims, liabilities, judgments, costs, and expenses based on Xerox's relative culpability. Xerox will not indemnify the University due to any negligent or willful act on the part of the University, its officers, employees, volunteers, or agents, or the negligent or willful acts of any party other than a Xerox officer, employee, or agent.

Article 15 (2). Service and Maintenance. Please note that the vast majority of on-site equipment repairs will be completed within 12 business hours. However, in the unlikely event that the repair time exceeds 12 business hours, Xerox agrees, as University's exclusive remedy, to issue an appropriate service credit for Xerox's failure to repair the equipment within the specified timeframe. The credit can be used to offset any invoice charge, excluding the Monthly Minimum Charge which is not subject to dispute.

Article 17. Risk of Loss. Please note that title to the Xerox supplied equipment will remain with Xerox until the University elects to purchase the equipment, and that the risk of the equipment's loss or damage will pass to the University upon delivery. The University is required to insure the equipment while installed. Title to the Lessor supplied equipment will remain with Lessor until University elects to purchase the equipment. Risk of the equipment's loss or damage will pass to the University upon delivery. University agrees that: (a) the equipment will remain personal property; (b) it will not attach the equipment as a fixture to any real estate; (c) it will not pledge, sub-lease, or part with possession of the equipment or file, or permit to be filed, any lien against the equipment; and, (d) it will not make any permanent alterations to the Equipment

Article 19.B Lessors Liability and Insurance Requirements. Xerox agrees to name the University as an additional insured under the comprehensive general liability and automobile liability insurance policies only for claims arising out of the willful or negligent acts, or omissions of Xerox in the performance of the services under the contract.

1. Comprehensive or Commercial Form General Liability Insurance Minimum Limits: Each occurrence \$2,000,000; 2. Products/Completed Operations \$2,000,000.
2. Business Auto Liability: Combined single limit of no less than \$3,000,000 per occurrence.

Certificates of insurance shall obligate Lessor's insurers to endeavor to notify University at least prior to cancellation of or material change in any of said insurance.

Attachment – University Appendix – Federal Government Contracts

Xerox provides 'commercial items,' as that term is defined in FAR Part 2. As such, Xerox is not subject to the cost principles of FAR Part 31, the Cost Accounting Standards, and the majority of the clauses listed in this attachment. We would be happy to comply with those clauses which the University and Xerox mutually agree apply to the acquisition of a commercial item

Appendix – Business Associate Agreement

Section 2(I) - Please note Xerox agrees to this section so long as the University grants Xerox 30 days' prior written notice to make its internal practices, books, and records, relating to the Use and Disclosure of PHI available to UC, and to the Secretary for purposes of determining University's compliance with HIPAA, HITECH and their implementing regulations.

Appendix – Data Security

Please note Xerox will not gain access to the University's Institutional Information or IT Resources in the course of providing the Goods/Services. Therefore, this Appendix is not applicable.

Appendix – General Data Protection Regulation

Please note Xerox offer does not include the processing of any personal data under the contract. Thus, the terms of this Appendix "General Data Protection Regulation" will not apply. In the event any of the provisions of this Appendix would apply, Xerox requests the following modifications:

C4. Xerox agreements with our subcontractors are confidential and its terms are subject to confidentiality provisions.

D3(i). Xerox requests the deletion of the word "pseudonymisation"

D5. In the event of any suspected or actual personal data breach, Xerox agrees to comply with security incident notification requirements within a reasonable time. Xerox respectfully requests the deletion of the sentence "but in no event more than two calendar days".

D7. Xerox requests University to replace "any data breach" language with "material data breach that cannot be remediated by Processor".

D12. Please note Xerox does not anticipate having access to any University's Data or have any data stored by Xerox during the course of its services. Xerox proposes to delete this provision as it is not applicable.

Addendum A, Scope of Processing Data as well as Addendum B, Standard Contractual Clause will be reviewed by Xerox on an engagement basis to determine its applicability.

Exhibit B – Administration Agreement Example (OMNIA)

Section 7. Xerox proposes to delete this section and modify it as follows: “7. NEITHER PARTY SHALL BE LIABLE IN ANY WAY TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY, PUNITIVE OR RELIANCE DAMAGES, EVEN IF THE OTHER PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.”

Section 12, Administrative Fee, Reporting and Payment.

Xerox agrees An “Administrative Fee” shall be defined and due to OMNIA Partners, Public Sector from Supplier in the amount of 3 percent (3%) (“Administrative Fee Percentage”) multiplied by the total monthly revenue billed by the Supplier for the sale of products and/or services to Principal Procurement Agency and Participating Public Agencies pursuant to the Master Agreement (as amended from time to time and including any renewal thereof) (“Contract Sales”). From time to time the parties may mutually agree in writing to a lower Administrative Fee Percentage for a specifically identified Participating Public Agency's Contract Sales.

To the extent the Supplier offers leasing or financing programs under the Master Agreement Contract to Participating Public Agencies itself or through a financing entity, Contract Sales under leasing or other financing programs shall be calculated using the net purchase price (the purchase price equivalent after trade-in allowances, etc.).

To the extent the Supplier offers trade-in allowance programs to Participating Public Agencies for transactions done under the Master Agreement Contract, Contract Sales shall be calculated using the net purchase price after the trade-in allowance.

Section 13. Please note Xerox agrees Contract Sales Reports for each calendar month shall be provided by Supplier to OMNIA Partners, Public Sector by the 45th day of the following month.

Section 15. Xerox agrees with this provision as stated with the exception of the last sentence and proposes this section be modified as follows: “15. Supplier will have thirty (30) days from the date of such notice to resolve the discrepancy to OMNIA Partners, Public Sector's reasonable satisfaction, including payment of any Administrative Fees due and owing, together with interest thereon in accordance with Section 13,”

Section 18. General Provisions.

Xerox requests this section be deleted in its entirety and replaced as follows: “18. Neither party may assign this Agreement without the prior written consent of the other party; provided, however, either party may assign the Agreement without prior written consent of the party in connection with the sale or transfer of substantially all of the assigning party's assets.”

END OF CLARIFICATIONS

Please refer to Xerox's clarifications to the University of California RFP on the embedded document.



2020 CA
Regentsofthe UnivofC



2020 CA
Regentsofthe UnivofC

Attachments

This section provides a list of the required supplier response documents to be returned with the RFP proposal and additional documentation, which supplements our response to University of California.

Descriptions
001881Feb 2020 Questionnaire.xlsx
Xerox UC Executive Summary.docx
Financials.pdf
References.pdf
Organization Chart.pdf
Account Management Team.docx
Delivery and Installation Capabilities.docx
VPAT AltaLink B8000 Series.pdf
VPAT AltaLink C8000 Series.pdf
VPAT VersaLink B405 Series.pdf
VPAT VersaLink B7000 Series.pdf
VPAT VersaLink C7020 / C7025 C7030.pdf
AltaLink B8045 / B8055 / B8065 / B8075 / B8090 RML.pdf
Environment Safety Facts.pdf
XOGFS-14U Xerox EPEAT and Certifications.pdf
Gabi Brochure 2020.pdf
Gabi Customer Expectation Doc.pdf
Xerox USB Keyboard.pdf
Gabi Voice Brochure.pdf
Scan Compression Brochure.pdf

Touchless Workplace Technologies.pdf

ConnectKey Brochure.pdf

XDM Diagram.pdf

ISO 27001 Certificate (Effective 2019 Expiry 2022) IS 514590.pdf

AltaLink C81XX B81XX Security Guide.pdf.

VersaLink Security Guide IAD-4.pdf

Xerox Workplace Suite Security Guide IAD.pdf

Xerox Device Manager Certification Guide 6.3.pdf

Security Incident Management Process.pdf

Xerox Security.pdf.

Pen Testing Attestation Letter.pdf

Service Guarantee Commitment and Credits.docx

Service Guarantee Commitment Requirements for Laser Printer.docx

TM Pricing.pdf

Xerox MFD UC Pricing Attachment.xlsx

Xerox MFD National Pricing.xlsx

Xerox Laser-Printer UC Pricing Attachment.xlsx

Xerox Laser-Printer National Pricing.xlsx

Xerox UC Additional Discounts Pricing Attachment.xlsx

Xerox Additional Discounts National Pricing.xlsx

Xerox UC Repair Parts Pricing Attachment.xlsx

Xerox Repair Parts National Pricing.xlsx

Xerox UC Accessory Sale Price List – All Accessories Available.xlsx

Xerox Price All Available Accessories National Pricing.xlsx

Xerox UC Equipment Lease Optional Accessories Pricing.xlsx

Xerox Optional Accessories National Pricing.xlsx

Xerox FMV UC Laser Printer Lease Pricing.xlsx

Xerox FMV Laser-Printer Lease National Pricing.xlsx

Xerox FPO UC Laser-Printer Lease Pricing Attachment.xlsx

Xerox UC OMNIA FPO Printer Lease Pricing.xlsx

Exhibit A Response for National Cooperative Contracts.docx.

Attachment A – List of all US Locations.zip

Attachment B – Xerox Dun & Bradstreet Report.pdf

Exhibit B – Administration Agreement.pdf

Exhibit F - Federal Funds Certifications.pdf

Exhibit G - New Jersey Business Compliance.pdf

Exhibit C – Master Intergovernmental Cooperative Purchasing Agreement.pdf

Exhibit D – Principal Procurement Agency Certificate.pdf

Exhibit E – Contract Sales Reporting Template.pdf

Exhibit H – Advertising Compliance Requirement.pdf

2020 CA Regents of the University of California Additional Terms Non UC OMNIA.docx.

2020 CA Regents of the University of California Additional Terms UC.docx.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

We have reviewed the University's Request for Proposal ("RFP") and have prepared the enclosed Purchase and Maintenance and 36, 48 and 60-months Lease Proposal (Fair Market Value, \$1 Buyout Option) subject to the University's contract standards or performance for your consideration. In addition, Xerox has also included a separate pricing and Terms & Conditions response for Non-University members subject to Omnia Partners contract standards of performance and terms and conditions. All operational requirements for the University in the contract, such as customized reporting and separately billed maintenance are applicable for University only. All operational requirements, performance standards and terms and conditions of the master agreement Xerox/Omnia contract are applicable for non-University customers. Although the Proposal is based on the requirements included in your RFP, our Proposal does include some responses that are slightly different. This document and our Proposal explain those differences. In addition, we have included some Additional Terms that were not addressed in the University's RFP. Please note that Xerox's Proposal is contingent upon the accuracy of the information included in the University's RFP and Xerox's review of the University's credit. Any material change to the information provided by the University, or the University's credit, may result in a change to Xerox's offer.

Please note that Xerox agrees to negotiate a solution that is acceptable to both parties if any of the below clarifications or Additional Terms are inconsistent with California law, or are otherwise unacceptable to the University. Our team is also prepared to discuss our Proposal in detail, and adjust our proposed equipment, support services, terms, and/or price offering based on the University's final requirements. Upon award of this RFP, Xerox agrees to negotiate a Contract that incorporates the mutually agreed terms contained in the University's RFP, our Proposal, Xerox's Purchase and Maintenance and Lease Agreement (applicable to the University and its affiliates), and OMNIA Partner's terms and conditions (applicable for Non-University members), and any additional negotiated item(s).

Xerox's Clarifications to the University's RFP

Xerox provides the following clarifications and comments to the below listed University RFP requirements.

RFP EVENT AND PROCESS SUMMARY

SECTION 3. MFD/PRINTER FLEET MANAGEMENT PROGRAMS; 3.1.1.1 MFD 36//48/60-months terms.

The Xerox Lease offering is based on a firm 36-month, 48-month and 60-month, FMV and \$1 Buy-out Option, of equipment installation commitment, and consists of a Monthly Base Charge that covers the cost of the equipment; the cost per copy and overage rates, any trade-in equipment refinanced / buyout amounts; an equipment trade-in credit value; the equipment's FOB shipment, freight, and inside delivery and removal (excluding any unique rigging expenses); the equipment's physical installation and connection to the University's network; and end user initial training, and the labor services detailed in our Proposal. Remote installations are also available where applicable.

Please note Xerox does not offer any trade bonuses for sale to lease equipment transactions under this Agreement. For competitive sale to sale trades Xerox will remove the competitive/owned equipment at Xerox expense.

SECTION 3. MFD/PRINTER FLEET MANAGEMENT PROGRAMS; 3.1.1.2 and 3.1.1.3 Discounts.

Outright Purchase Equipment. Please note Xerox will provide an additional 5% discount on the published University equipment mainframe price (excluding accessories) list for Outright Sale/FMV & FPO Lease (equipment price only, excluding maintenance) for orders for Managed Programs. Any/all discounts will be taken at the time of order.

Lease Equipment. Please note Xerox cannot guarantee any additional discounts beyond the published lease price however, Xerox will review/consider these opportunities for additional discounts for "Managed Programs" upon request.

SECTION 4. PRODUCT CERTIFICATION

Equipment provided under the Contract is currently manufactured by Xerox, though the equipment may contain recycled components that have been reprocessed to meet Xerox' new parts performance standards. The County will be the first user of the equipment.

SECTION 5. PROGRAM FOR TRADE-INS/UPGRADES

Trade-In Equipment. Xerox warrants that University has the right to transfer title to the Equipment University is trading in as part of an Order ("Trade-In Equipment"), and that the Trade-In Equipment is in good working order and has not been modified from its original configuration (other than by Xerox). Title and risk of loss to the Trade-In Equipment will pass to Xerox when Xerox removes the Trade-In Equipment from University premises. University will maintain the Trade-In Equipment at its present site and in substantially the Trade-In Equipment's present condition until removed by Xerox. University will pay all

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

accrued charges for the Trade-In Equipment, up to and including payment of the final principal payment number and all applicable maintenance, administrative, supply and finance charges until Xerox removes the Trade-In Equipment from the University's premises.

Upgrades. Xerox's Purchase and Maintenance as well as Xerox Lease offer allows the University to place additional equipment mainframe orders at the same quoted contract price throughout the 60-month master agreement term, provided each additional equipment placement remains installed for a minimum 36/48/60-month term. Xerox will also provide a separate price quote if the University desires to acquire additional equipment having an installation term less than 60-months. The equipment's features and performance can also be upgraded through the addition of a number of optional accessories. Accessory options included with the mainframe can be obtained at the contract quoted price. Any accessory ordered following the mainframe's installation will have the price readjusted based on the mainframe's remaining agreement term. Please remember that the Xerox Purchase and Maintenance as well as Xerox Lease offering is based on a firm 36/48/60-month equipment installation term that can only be terminated due to fiscal year funds non-appropriation or an uncured performance failure. If the equipment is cancelled for the University's convenience and not replaced, or traded to a different unit, the University will be assessed a liquidated damages charge. In order to avoid this charge, Xerox recommends that the equipment either be: (a) exchanged with another University unit, or (b) moved to another University location and replaced with a unit that fits the end users current work requirements.

D. Organizational Context.

University of California Pricing Terms - For University of California and affiliates Xerox agrees to extend the specific University product pricing and terms of this Agreement.

OMNIA Partners' National Master Agreement— Xerox agrees to make resulting OMNIA Partners' pricing/terms from this solicitation available to other public agencies nationally, including state and local governmental entities, public and private primary, secondary and higher education entities, non-profit entities, and agencies for the public benefit ("Public Agencies") through OMNIA Partners' Cooperative purchasing program so long as such Public Agency is a registered member at OMNIA. Non-University OMNIA members will procure equipment and services subject to the terms and conditions of the OMNIA Master Agreement which terms are hereby incorporated by their reference <https://www.sourcewell-mn.gov/cooperative-purchasing/083116-xox?domain=870%20%20%20%20%20%20%20%20%20%20%20%20%20%D0%B5H#tab-contract-documents>

3 MFD/Printer Fleet Management Programs - Delivery and Installation.

Delivery. Please note the following will apply to any Purchase and Lease transaction: Unless otherwise agreed upon by the parties, Xerox equipment deliveries can normally be expected within ten business days following the receipt of the University's equipment approved and accepted purchase order, except during times of product constraint. Xerox will inform the University if a constraint condition exists and will provide a revised delivery date. If the revised target delivery date is unacceptable, the University can cancel the order without penalty to either party.

Installation. Unless the Purchase and Maintenance and Lease Agreement is preceded by a Trial order, the equipment will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

2.2 Equipment Service and Support

Uptime. Total Uptime Xerox's Uptime objective is to maintain an average 96% equipment uptime performance based on a three-month rolling average for the University's entire Xerox-branded equipment population that is operated with the equipment's operating guideline for the specified product. Uptime is calculated as follows:

1. **UPTIME TARGET.** Provided Customer has at least twenty-five (25) units of Equipment installed under this Agreement, Xerox agrees to maintain an Uptime Target for the total Equipment population installed under this Agreement, which shall be measured as provided below over a three (3) calendar month rolling period, of at least ninety-six percent (96%) in the aggregate for the Equipment subject to this Agreement that is operated within the specified Maximum Monthly Volume Range, (to be included upon University's request in an Appendix to this Contract) and installed within twenty-five (25) miles of a Xerox service location. This Uptime Target commences on the first day of the calendar month that begins at least one hundred twenty (120) days after the Agreement commences.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

2. **CONTRACTED PERIOD OF COVERAGE.** Xerox will provide Maintenance Services, as the same is set forth in this Agreement, during Customer's normal business hours Contracted Period of Coverage ("CPOC"), which shall be defined as 9:00 a.m. to 5:00 p.m., Local Time, Mondays through Fridays (excluding Xerox-recognized holidays), for the purposes of this Agreement.

3. **UPTIME HOURS DEFINITION.** "Uptime Hours" equals the number of hours per calendar month that the Equipment is available for use. For this Agreement, Uptime Hours equals 567 hours per three (3) calendar months and has been calculated by multiplying the number of hours per day in the CPOC times the average number of days per three (3) calendar month period such coverage is provided, which, for the purposes of this Agreement, is sixty-three (63) days per three (3) calendar month period..

4. **DOWNTIME HOURS DEFINITION.** "Downtime Hours" shall mean the number of hours in any three (3) calendar month period during which Equipment maintained hereunder is inoperative (i.e., cannot make any copies or prints, as applicable) during the CPOC, including machine-repair time and response time when the Equipment is inoperative. Downtime Hours do not include time when the Equipment's inoperability is due to user misuse or abuse of the Equipment, Customer's negligence or intentional acts, fire, environmental failure at the installation site or use of the Equipment in a manner other than was intended; preventative maintenance, Equipment relocation or inspections are being performed; and, time taken in producing usable copies or prints.

5. **CALCULATION.** The Uptime Percentage Rate for a given calendar month is calculated as follows:

$$\text{Uptime Percentage Rate} = \frac{\text{CPOC } (567) - \text{Downtime Hours } (x)}{\text{CPOC Hours } (567)}$$

Laser Printers.

Lease: For FMV/FPO leases the Maintenance is included and begins upon install.

Response/Repair Time. Xerox's response time objective is to return all service calls within one business hour, and to arrive on-site on average within 3.5 to 4 business hours for multifunction color devices, if the problem cannot be resolved over the phone. Response Time for other devices will be provided upon request. Response time is calculated based on the quarterly response time average for the University's entire Xerox-branded equipment population. Calls can be placed toll free 24-business hours per day, 7 days per week, and 365 days a year. During standard business hours (8 A.M. to 5 P.M., Monday thru Friday), all service calls will be directed to our Service Welcome Center where our service personnel will attempt to resolve the issue over the phone through on-line diagnostics. If the problem cannot be resolved over the phone the representative will provide the caller with the technicians estimated time of arrival. The Service Technician will contact the caller prior to arriving on-site to discuss the problem and determine if they have the appropriate parts, or if there will be a change to the arrival time. Evening, weekend, and holiday phone service is also available. On-site evening, weekend, and holiday service support can also be prearranged or may be available based on evening resource availability. The 24x7-call center and business hour technical support is included in our contract offering. After hour, weekend, and holiday on-site technical support is available at Xerox's then current overtime rate. Please refer to the XPS Description of Services for response time objectives relating to the XPS / Managed Print Services offering.

Delivery/Installation.

Delivery. Please note the following will apply to any Purchase and Lease transaction: Unless otherwise agreed upon by the parties, Xerox equipment deliveries can normally be expected within ten business days following the receipt of the University's equipment approved purchase order, except during times of product constraint. Xerox will inform the University if a constraint condition exists and will provide a revised delivery date. If the revised target delivery date is unacceptable, the University can cancel the order without penalty to either party.

Installation. Unless the Purchase and Maintenance and Lease Agreement is preceded by a Trial order, the equipment will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

Attachment – University Terms and Conditions of Purchase

Article 2. Term and Termination.

Xerox recognizes the University's right to terminate the Agreement for its convenience due to a change in its business needs. However, the Xerox offer is based on a firm 36, 48, or 60-month equipment installation commitment, and cannot be terminated except for fiscal year funds non-appropriation or uncured Xerox default.

In order to terminate the Agreement due to non-appropriation, University must provide Supplier with written notice, within 31-days of its governing body's decision not to appropriate funds, stating that the University's governing body failed to appropriate funds. The notice must certify that the canceled equipment is not being replaced by equipment performing similar functions during the ensuing fiscal year. In addition, the University will be required to return the equipment to Supplier with transportation costs borne by Supplier. The University will then be released from its obligation to make any further payments beyond those through the end of the last fiscal year for which funds have been appropriated.

University may terminate this Agreement for convenience at any time, in whole or in part, in accordance with the terms of Article 2 of University of California Terms and Conditions of Purchase. In the event of such termination, University agrees to provide Xerox at least thirty (30) days prior written notice of the effective date of termination and the extent thereof, such termination shall not affect any leased unit that has not fulfilled the appropriate term.

If any termination of this Agreement takes place, Xerox shall extend to University, upon University request, an additional ninety (90) day period to properly implement a smooth transition. Fees for the services performed during the additional ninety (90) days will be in good faith negotiated between University and Xerox. Termination under this provision, shall not apply to orders received by Xerox prior to the effective date of termination.

In the event Xerox cannot or does not perform its obligations, University reserves the right to terminate the Agreement. If within thirty (30) days of receipt of written notice from University of Xerox's breach of any term or condition of the Agreement, Xerox shall fail to remedy such breach, then University may terminate the Agreement. However, this cancellation provision does not pertain to any leased equipment installed prior to University's termination notice. In the event the Agreement is terminated, individual lease placements will continue until their scheduled expiration date, and continue to be governed by, and be subject to, the terms and conditions of the individual lease and the Agreement.

Article 3. Pricing, Invoicing Method, and Settlement Method and Terms. Xerox will not issue an invoice until Services have been rendered and accepted. University will pay Xerox, within thirty-one (31) days of receipt of an undisputed and accurate invoice. The agreed upon minimum lease payment will not be subject to dispute at any time. Xerox will not issue an invoice until Services have been rendered and accepted.

Article 4. Inspection. Xerox can support the University's inspection and acceptance requirement by initially installing the equipment under a Trial arrangement. Unless an order is preceded by a Trial order, the Services will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

Article 6.j Outsourcing (Public Contract Code Section 12147 Compliance). All services included in the Xerox bid to be specifically contracted for by the University will be provided within the U.S. However, certain back-office contract administration and customer support services are performed by Xerox and/or its affiliates from locations outside the U.S.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

Article 7. Intellectual Property. Xerox does not anticipate the development of any customized products or programming in connection with the services provided under the Contract. Xerox agrees that all University authored documents printed/copied on Xerox supplied equipment is the University's sole and exclusive property, and that Xerox shall have no rights to these documents. Also, all Xerox generated reports and the output of Services is Customer's sole and exclusive property and Xerox will have no rights to these documents or data, except as may be required for Xerox to perform Services. All other work prepared by or processes developed by Xerox for the University's use will remain the sole property of Xerox and is not deemed a "work for hire". However, Xerox grants the University a non-exclusive, perpetual, fully paid-up, world wide right to use, display, reproduce, and modify any report, form, design, computer programs, code, or other work of authorship provided by Xerox to the University in the course of performing the Services under the Contract strictly for the University's internal business use and not for resale or distribution outside of the University's organization.

Article 8. Indemnity and Liability.

Indemnification is contingent upon University giving Xerox written notice, by registered mail, promptly after it becomes aware of any claim to be indemnified hereunder and permits Xerox to control the defense of any such claim or action and Xerox's own expense. Notice shall be sent to "Corporate Risk, Xerox Corporation, Long Ridge Road, Stamford, Connecticut, 06940." University agrees that Xerox may employ attorneys of its own choice to appear and defend the claim or action and that University shall do nothing to compromise the defense of such claim or action or any settlement thereof and shall provide Xerox with all reasonable assistance which Xerox may require. Xerox shall not be obligated to indemnify the University against the University's own acts or omissions.

Except for indemnified matters and to the extent permitted by applicable law, all other liability of Xerox to University for damages of any kind of type, including but not limited to indirect, consequential, incidental, or special damages, arising from Xerox performance or failure to perform under this Contract or by virtue of Xerox's tortious conduct (including negligence whether passive or active) shall be limited to the amounts paid by University under this Agreement. Provided, however, that the foregoing limitation of liability shall not apply to claims by University for personal injury or damage to real or tangible property caused by Xerox's negligence.

Article 9. Insurance. Xerox agrees to include the University as an additional insured under the comprehensive general liability and automobile liability insurance policies only for claims arising out of the willful or negligent acts, or omissions of Xerox in the performance of the services under the contract. Xerox and University will agree on the final coverage required under this Proposal.

Article 17. Additional Terms Applicable to the Furnishing of Goods

A. Price Decreases.

Xerox agrees immediately to notify the University of any price decreases from its suppliers, and to pass through to UC any price decreases. Any price reduction resulting from this provision shall only apply to orders received after the effective date of the price reduction.

B. Title. Title to the Goods purchased under the Agreement, along with the risk of equipment's loss or damage, will pass directly from Xerox to University upon delivery, subject to University's right to reject upon inspection.

Article 20. Prohibition on Unauthorized Use or Disclosure of Institutional Information; (e) No Offshoring.

All services included in the Xerox bid to be specifically contracted for by the University will be provided within the U.S. However, certain back-office contract administration and customer support services are performed by Xerox and/or its affiliates from locations outside the U.S.

Article 27. Force Majeure. This provision does not relieve either party of its obligation to make payments due under the Contract. Any University purchases to procure the services from other sources without Xerox's prior approval will be at the University's expense.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

Attachment – University Terms and Conditions of Equipment Lease

Article 2. Inspection. Xerox can support the University's inspection and acceptance requirement by initially installing the equipment under a Trial arrangement. Unless an order is preceded by a Trial order, the Services will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

Article 5. Termination. Xerox recognizes the University's right to terminate the Agreement for its convenience due to a change in its business needs. However, the Xerox offer is based on a firm 36, 48, or 60-month equipment installation commitment, and cannot be terminated except for fiscal year funds non-appropriation or uncured Xerox default.

The initial term for any individual lease order will be the number of full calendar months stated in the order. The minimum lease payment for any partial month following the equipment installation date will be billed on a pro rata basis, based on a 31-day month. The term for each unit of equipment will commence upon the delivery of customer-installable equipment; or the installation of Xerox-installable equipment and will expire on the last day of the final full calendar month of the contracted term indicated in the order.

University may at its option, by written notice stating the extent and effective date, terminate this order at the anniversary date of the lease or at the end of any fiscal year in whole or in part in the event the funding agency does not appropriate sufficient funds to continue the lease payments.

In order to terminate the Agreement due to funding non-appropriation, the University must provide Xerox with written notice, within 30-days of its governing body's decision not to appropriate funds, stating that the University's governing body failed to appropriate funds. In addition, the University will be required to return the equipment to Xerox with transportation costs borne by Xerox. The University will then be released from its obligation to make any further payments beyond those through the end of the last fiscal year for which funds have been appropriated. Other than as stated above, leases may not be cancelled prior to expiration. Early cancellation of individual leases without cause or cancellation of individual leases by Xerox due to the University's material breach will result in an early termination charge that is equal to the sum of the remaining payments less any unearned maintenance and supply charges discounted at 4% per annum. In no event shall the amount paid exceed the total contracted price, minus payments already made.

Xerox will provide University with no less than thirty-one (31) days advance notice of the expiration of each lease term. Upon lease expiration, University shall have the option to:

- Purchase the equipment AS IS, WHERE IS, by giving Xerox at least thirty (30) days prior notice of University intent to purchase at the termination of the term specified in any order or any renewal thereof. The purchase option price for FMV leases shall be the equipment's then fair market value plus all applicable sales taxes. The purchase option for FPO will be \$1 plus all applicable sales taxes.
- Lease the current equipment at the same monthly price on a month-to-month basis. This type of lease extension may be cancelled without penalty upon 30 days written notice.
- Have Xerox provide a quote on a new 12- or 24-month lease on the current equipment. This will yield a lower monthly price; however, the University would not be able to cancel the lease without termination charges until expiration of the new extended lease.

Upon expiration of a lease without extension, University will make the equipment available for removal by Xerox at Xerox's cost. At the time of removal, the equipment will be in the same condition as when delivered, reasonable wear and tear accepted.

A lease order under the contract is a "finance lease" under Article 2A of the Uniform Commercial Code and, except to the extent expressly provided under the Contract, and to the extent permitted by California law, Customer waives all rights and remedies conferred upon a lessee by Article 2A.

Article 6. Title. Title to the Goods purchased under the Agreement, along with the risk of equipment's loss or damage, will pass directly from Xerox to University upon delivery, subject to University's right to reject upon inspection.

Article 11. Proprietary Rights Indemnity. Xerox will agree to this indemnity provision providing Xerox is given written notice of the claim or action and allowed to select attorneys of its own choice to appear and defend the claim or action. In addition, the University agrees to provide Xerox with all reasonable assistance that Xerox may require, and that the University will do nothing

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

to compromise Xerox's defense or settlement of the claim or action. Xerox agrees that it will be responsible for its equitable share of any claims, liabilities, judgments, costs, and expenses based on Xerox's relative culpability. Xerox will not indemnify the University due to any negligent or willful act on the part of the University, its officers, employees, volunteers, or agents, or the negligent or willful acts of any party other than a Xerox officer, employee, or agent.

Article 15 (2). Service and Maintenance. Please note that the vast majority of on-site equipment repairs will be completed within 12 business hours. However, in the unlikely event that the repair time exceeds 12 business hours, Xerox agrees, as University's exclusive remedy, to issue an appropriate service credit for Xerox's failure to repair the equipment within the specified timeframe. The credit can be used to offset any invoice charge, excluding the Monthly Minimum Charge which is not subject to dispute.

Article 17. Risk of Loss. Please note that title to the Xerox supplied equipment will remain with Xerox until the University elects to purchase the equipment, and that the risk of the equipment's loss or damage will pass to the University upon delivery. The University is required to insure the equipment while installed. Title to the Lessor supplied equipment will remain with Lessor until University elects to purchase the equipment. Risk of the equipment's loss or damage will pass to the University upon delivery. University agrees that: (a) the equipment will remain personal property; (b) it will not attach the equipment as a fixture to any real estate; (c) it will not pledge, sub-lease, or part with possession of the equipment or file, or permit to be filed, any lien against the equipment; and, (d) it will not make any permanent alterations to the Equipment

Article 19.B Lessors Liability and Insurance Requirements. Xerox agrees to name the University as an additional insured under the comprehensive general liability and automobile liability insurance policies only for claims arising out of the willful or negligent acts, or omissions of Xerox in the performance of the services under the contract.

1. Comprehensive or Commercial Form General Liability Insurance Minimum Limits: Each occurrence \$2,000,000; 2. Products/Completed Operations \$2,000,000.
2. Business Auto Liability: Combined single limit of no less than \$3,000,000 per occurrence. Certificates of insurance shall obligate Lessor's insurers to endeavor to notify University at least prior to cancellation of or material change in any of said insurance.

Attachment – University Appendix – Federal Government Contracts

Xerox provides 'commercial items,' as that term is defined in FAR Part 2. As such, Xerox is not subject to the cost principles of FAR Part 31, the Cost Accounting Standards, and the majority of the clauses listed in this attachment. We would be happy to comply with those clauses which the University and Xerox mutually agree apply to the acquisition of a commercial item

Appendix – Business Associate Agreement

Section 2(l) - Please note Xerox agrees to this section so long as the University grants Xerox 30 days' prior written notice to make its internal practices, books, and records, relating to the Use and Disclosure of PHI available to UC, and to the Secretary for purposes of determining University's compliance with HIPAA, HITECH and their implementing regulations.

Appendix – Data Security

Please note Xerox will not gain access to the University's Institutional Information or IT Resources in the course of providing the Goods/Services. Therefore, this Appendix is not applicable.

Appendix – General Data Protection Regulation

Please note Xerox offer does not include the processing of any personal data under the contract. Thus, the terms of this Appendix "General Data Protection Regulation" will not apply. In the event any of the provisions of this Appendix would apply, Xerox requests the following modifications:

C4. Xerox agreements with our subcontractors are confidential and its terms are subject to confidentiality provisions.

D3(i). Xerox requests the deletion of the word "pseudonymisation"

D5. In the event of any suspected or actual personal data breach, Xerox agrees to comply with security incident notification requirements within a reasonable time. Xerox respectfully requests the deletion of the sentence "but in no event more than two calendar days".

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

D7. Xerox requests University to replace "any data breach" language with "material data breach that cannot be remediated by Processor".

D12. Please note Xerox does not anticipate having access to any University's Data or have any data stored by Xerox during the course of its services. Xerox proposes to delete this provision as it is not applicable.

Addendum A, Scope of Processing Data as well as Addendum B, Standard Contractual Clause will be reviewed by Xerox on an engagement basis to determine its applicability.

Exhibit B – Administration Agreement Example (OMNIA)

Section 7. Xerox proposes to delete this section and modify it as follows: "7. NEITHER PARTY SHALL BE LIABLE IN ANY WAY TO THE OTHER FOR ANY SPECIAL, INCIDENTAL, INDIRECT, CONSEQUENTIAL, EXEMPLARY, PUNITIVE OR RELIANCE DAMAGES, EVEN IF THE OTHER PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES."

Section 12, Administrative Fee, Reporting and Payment.

Xerox agrees An "Administrative Fee" shall be defined and due to OMNIA Partners, Public Sector from Supplier in the amount of 3 percent (3%) ("Administrative Fee Percentage") multiplied by the total monthly revenue billed by the Supplier for the sale of products and/or services to Principal Procurement Agency and Participating Public Agencies pursuant to the Master Agreement (as amended from time to time and including any renewal thereof) ("Contract Sales"). From time to time the parties may mutually agree in writing to a lower Administrative Fee Percentage for a specifically identified Participating Public Agency's Contract Sales.

To the extent the Supplier offers leasing or financing programs under the Master Agreement Contract to Participating Public Agencies itself or through a financing entity, Contract Sales under leasing or other financing programs shall be calculated using the net purchase price (the purchase price equivalent after trade-in allowances, etc.).

To the extent the Supplier offers trade-in allowance programs to Participating Public Agencies for transactions done under the Master Agreement Contract, Contract Sales shall be calculated using the net purchase price after the trade-in allowance.

Section 13. Please note Xerox agrees Contract Sales Reports for each calendar month shall be provided by Supplier to OMNIA Partners, Public Sector by the 45th day of the following month.

Section 15. Xerox agrees with this provision as stated with the exception of the last sentence and proposes this section be modified as follows: "15. Supplier will have thirty (30) days from the date of such notice to resolve the discrepancy to OMNIA Partners, Public Sector's reasonable satisfaction, including payment of any Administrative Fees due and owing, together with interest thereon in accordance with Section 13,"

Section 18. General Provisions.

Xerox requests this section be deleted in its entirety and replaced as follows: "18. Neither party may assign this Agreement without the prior written consent of the other party; provided, however, either party may assign the Agreement without prior written consent of the party in connection with the sale or transfer of substantially all of the assigning party's assets."

END OF CLARIFICATIONS

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

ADDITIONAL TERMS

These additional terms are incorporated into the Xerox Proposal and are in addition to the terms included in the University's RFP. Should there be a conflict between the various provisions the order of precedence shall be these Additional Terms followed by the University's RFP.

TERMS APPLIABLE TO THE UNIVERSITY OF CALIFORNIA AND ITS AFFILIATES

The following additional terms will apply to the University of California and its affiliates:

GENERAL TERMS

1. **CONSUMABLE SUPPLIES.** If "Consumable Supplies" is identified in Maintenance Plan features, Maintenance Services will include black toner and/or solid ink and color toner and/or solid ink, if applicable ("Consumable Supplies"). Highlight color toner, clear toner, and custom color toner are excluded. Depending on the Equipment model, Consumable Supplies may also include developer, fuser agent, imaging units, waste cartridges, transfer rolls, transfer belts, transfer units, belt cleaner, staples, maintenance kits, print Cartridges, drum Cartridges, waste trays and cleaning kits. Consumable Supplies are Xerox's property until used by you, and you will use them only with the Equipment for which "Consumable Supplies" is identified in Maintenance Plan Features. If Consumables Supplies are furnished with recycling information, Customer will return the used item to Xerox for remanufacturing. Shipping information is available at Xerox.com/GWA. Upon expiration of this Agreement, Customer will include any unused Consumable Supplies with the Equipment for return to Xerox at the time of removal. If your use of Consumable Supplies exceeds Xerox's published yield by more than 10%, Xerox will notify you of such excess usage. If such excess usage does not cease within 30 days after such notice, Xerox may charge you for such excess usage. Upon request, you will provide current meter reads and/or an inventory of Consumable Supplies in your possession.
2. **CARTRIDGES.** If Xerox is providing Maintenance Services for Equipment utilizing cartridges designated by Xerox as customer replaceable units, including copy/print cartridges and xerographic modules or fuser modules ("Cartridges"), you agree to use only unmodified Cartridges purchased directly from Xerox or its authorized resellers in the U.S. Cartridges packed with Equipment and replacement Cartridges may be new, remanufactured or reprocessed. Remanufactured and reprocessed Cartridges meet Xerox's new Cartridge performance standards and contain new or reprocessed components. To enhance print quality, Cartridge(s) for many models of Equipment have been designed to cease functioning at a predetermined point. In addition, many Equipment models are designed to function only with Cartridges that are newly manufactured original Xerox Cartridges or with Cartridges intended for use in the U.S.
3. **"Guarantee Period"** means the period commencing 90 days after installation of the Equipment to 18 months after installation of the Equipment. For the Guarantee Period, if the Equipment is not performing substantially consistent with the performance expectations outlined in the Customer Expectations Document ("CED") or such other documentation provided with the Equipment if a CED does not accompany the Equipment (the "Documentation"), Xerox will, after attempting to repair the device per the Maintenance Services provision hereto and upon University's request but in Xerox's sole discretion, replace such Equipment without charge with identical Equipment or with other Equipment with comparable features and capabilities (the "Equipment Guarantee"). This Equipment Guarantee applies only to Equipment that has been (a) continuously maintained by Xerox per a contract with Xerox, and (b) operated at all times in accordance with the CED or Documentation. The Equipment Guarantee does not apply to certain Equipment, which models shall be identified in your applicable order-related documents. Except as otherwise stated in an order-related document, this Equipment Guarantee replaces and supersedes any other guarantee from Xerox, whether made orally or in writing, styled a "Total Satisfaction Guarantee", "Satisfaction Guarantee" or otherwise covering the subject matter set forth above.
4. **NON-APPROPRIATION OF FUNDS.** The continuation of any lease, rental purchase or maintenance agreement will be subject to, and contingent upon, sufficient funds being made available by the Purchasing Entity local source, State Legislature and/or federal sources. The Purchasing Entity may terminate any such lease or rental agreement, and Awarded Vendor waives any and all claim(s) for damages, effective immediately upon receipt of written notice (or any date specified therein) if for any reason the Purchasing Entity's funding sources are not available.
5. **LIMITATION OF LIABILITY.** For claims arising out of or relating to this Agreement, whether the claim alleges tortious conduct (including negligence) or any other legal theory, but excepting liability under the indemnification obligations set forth

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

in this Agreement, Xerox will not be liable to you for any direct damages in excess of \$10,000 or the amounts paid hereunder, whichever is greater, and neither party will be liable to the other for any special, indirect, incidental, consequential or punitive damages. Any action you take against Xerox must be commenced within 2 years after the event that caused it.

6. **WARRANTY DISCLAIMER.** XEROX DISCLAIMS THE IMPLIED WARRANTIES OF NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE AND, FOR THIRD PARTY PRODUCTS, THE IMPLIED WARRANTY OF MERCHANTABILITY.
7. **REMOTE SERVICES.** Certain models of Equipment are supported and serviced using data that is automatically collected by Xerox or transmitted to or from Xerox by the Equipment connected to Customer's network ("Remote Data") via electronic transmission to a secure off-site location ("Remote Data Access"). Remote Data Access also enables Xerox to transmit to Customer Releases for Software and to remotely diagnose and modify Equipment to repair and correct malfunctions. Examples of Remote Data include product registration, meter read, supply level, Equipment configuration and settings, software version, and problem/fault code data. Remote Data may be used by Xerox for billing, report generation, supplies replenishment, support services, recommending additional products and services, and product improvement/development purposes. Remote Data will be transmitted to and from Customer in a secure manner specified by Xerox. Remote Data Access will not allow Xerox to read, view or download the content of any Customer documents or other information residing on or passing through the Equipment or Customer's information management systems. Customer grants the right to Xerox, without charge, to conduct Remote Data Access for the purposes described above. Upon Xerox's request, Customer will provide contact information for Equipment such as name and address of Customer contact and IP and physical addresses/locations of Equipment. Customer will enable Remote Data Access via a method prescribed by Xerox, and Customer will provide reasonable assistance to allow Xerox to provide Remote Data Access. Unless Xerox deems Equipment incapable of Remote Data Access, Customer will ensure that Remote Data Access is maintained at all times Maintenance Services are being performed.

SOFTWARE

8. Software License

Xerox may provide Software to Customer pursuant to an Order hereunder. The following license applies to Software provided hereunder, unless such Software is accompanied by a click-wrap or shrink-wrap license agreement or otherwise provided subject to a separate license agreement.

- a. Xerox grants Customer a non-exclusive, non-transferable, non-assignable (by operation of law or otherwise) license to use in the U.S.: (i) Base Software only on or with the Equipment with which (or within which) it was delivered; and (ii) Application Software only on any single unit of Equipment, subject to Customer remaining current in the payment of any indicated applicable Software license fees (including any annual renewal fees). For Services Software, Xerox grants Customer a non-exclusive, non-transferable, non-assignable (by operation of law or otherwise) license in the U.S. to install the Services Software on a host computer(s) or server(s) or, if applicable, on Equipment or Third Party Hardware, and, further, if applicable, on the number of workstations, laptops and mobile devices specified in the Order, and to use the Services Software only for the purpose of receiving the applicable Services. Customer has no other rights to the Software. Customer will not and will not allow its employees, agents, contractors or vendors to: (i) distribute, copy, modify, create derivatives of, decompile, or reverse engineer Software except as permitted by applicable law; (ii) activate Software delivered with or within the Equipment in an un-activated state; or, (iii) access or disclose Diagnostic Software for any purpose. Title to Software and all copyrights and other intellectual property rights in Software will reside solely with Xerox and its licensors (who, if required by the terms of the third party license agreement with Xerox, will be considered third party beneficiaries of this Agreement's software and limitation of liability provisions).
- b. The Base Software license will terminate, as applicable: (i) if Customer no longer uses or possesses the Equipment with which the Base Software was provided; or (ii) upon the expiration or termination of any Order under which Customer has acquired the Equipment with which the Base Software was provided (unless Customer has exercised an option to purchase the Equipment, where available, in which case the license to Base Software is perpetual and transferrable with purchase of the Equipment by Customer).
- c. Software may contain code to prevent its unlicensed use and/or transfer. If Customer does not permit Xerox periodic access to such Software, this code may impair the Equipment's and/or Software's functionality.
- d. Xerox does not warrant that the Software will be free from errors or that its operation will be uninterrupted.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

9. SOFTWARE SUPPORT

- a. Software support will be provided by Xerox or a designated service provider as follows. For Base Software, Software support will be provided during the initial term of the applicable Order and any renewal period, but not longer than 5 years after Xerox stops taking orders for the subject model of Equipment. For Application Software, Software support will be provided as long as Customer is current in the payment of all applicable software license, annual renewal and "support only" fees. For Services Software, support will be provided in accordance with the terms of the applicable Statement of Work or Order.
- b. Xerox will maintain a web-based or toll-free hotline during Xerox's standard working hours to report Software problems and answer Software-related questions. Xerox, either directly or with its vendors, will make reasonable efforts to: (i) assure that Software performs in material conformity with its Documentation; (ii) provide available workarounds or patches to resolve Software performance problems; and (iii) resolve coding errors for (1) the current release and (2) the previous release for a period of 6 months after the current release is made available to Customer. Xerox will not be required to provide Software support if Customer has modified the Software.
- c. Xerox may make available new releases of the Software that are designated as "Maintenance Releases" or "Updates." Maintenance Releases or Updates are provided at no charge and must be implemented within 6 months after being made available to Customer. Each Maintenance Release or Update shall be considered Software governed by these terms. Feature Releases will be subject to additional license fees at Xerox's then-current pricing and shall be considered Software governed by these terms and conditions (unless otherwise noted in an Order). Implementation of a Maintenance Release, Update or Feature Release may require Customer to procure, at its expense, additional hardware and/or software from Xerox or another entity. Upon installation of a Maintenance Release, Update or Feature Release, Customer will return or destroy all prior Maintenance Releases, Updates or Feature Releases.
- d. Xerox may increase Software license fees and support fees for Application Software annually by an amount no greater than the CPI Adjustment Percentage.

10. DIAGNOSTIC SOFTWARE

Diagnostic Software and method of entry or access to it constitute valuable trade secrets of Xerox. Title to the Diagnostic Software shall at all times remain solely with Xerox and Xerox's licensors. Xerox does not grant Customer a license or right to use the Diagnostic Software. Customer will not use, reproduce, distribute, or disclose the Diagnostic Software for any purpose (or allow third parties to do so). Customer will allow Xerox reasonable access to the Equipment during Customer's normal business hours to remove or disable Diagnostic Software if Customer is no longer receiving Maintenance Services from Xerox.

11. THIRD PARTY SOFTWARE

Third Party Software is subject to license and support terms provided by the applicable Third Party Software vendor.

12. **DATA SECURITY.** Certain models of Equipment can be configured to include a variety of data security features. There may be an additional cost associated with certain data security features. The selection, suitability and use of data security features are solely Customer's responsibility. Upon request, Xerox will provide additional information to Customer regarding the security features available for particular Equipment models.

LEASE TERMS AND CONDITIONS

13. **PRODUCTS.** "Products" means the equipment ("Equipment"), Software and supplies identified in this Agreement. the University agrees the Products are for the University's business use (not resale) in the United States and its territories and possessions ("U.S.") and will not be used for personal, household or family purposes.
14. **MAINTENANCE SERVICES.** Except for Equipment and/or Third Party Hardware identified as "No Svc.", Xerox (or a designated servicer) will keep the Equipment and/or Third Party Hardware in good working order ("Maintenance Services"). The provision of Maintenance Services is contingent upon Customer facilitating timely and efficient resolution of Equipment and/or Third Party Hardware issues by: (a) utilizing Customer-implemented remedies provided by Xerox; (b) replacing Cartridges; and (c) providing information to and implementing recommendations provided by Xerox telephone support personnel. If an Equipment and/or Third Party Hardware issue is not resolved after completion of (a) through (c) above, Xerox will provide on-site support as provided herein. Maintenance Services will be provided during Xerox's standard working hours in areas open for repair service for the Equipment and/or Third Party Hardware. Maintenance Services excludes repairs due to: (i) misuse, neglect or abuse; (ii) failure of the installation site or the PC or workstation used with the Equipment and/or Third Party Hardware to comply with Xerox's published specifications or Third Party Hardware vendor's published specifications, as applicable; (iii) use of options, accessories or products not serviced by

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

Xerox; (iv) non-Xerox alterations, relocation, service or supplies; or (v) failure to perform operator maintenance procedures identified in operator manuals. Replacement parts may be new, reprocessed or recovered and all replaced parts become Xerox's property. Xerox will, as your exclusive remedy for Xerox's failure to provide Maintenance Services, replace the Equipment with an identical model or, at Xerox's option, another model with comparable features and capabilities. There will be no additional charge for the replacement Equipment during the remainder of the initial Term. If meter reads are a component of your Equipment's Maintenance Plan, you will provide them using the method and frequency identified by Xerox. If you do not provide a meter reading for Equipment not capable of Remote Data Access, or if Remote Data Access is interrupted, Xerox may estimate the reading and bill you accordingly. For Third Party Hardware identified as "No Svc.", you shall enter into a maintenance agreement with the Third Party Hardware vendor or its maintenance service provider, who shall be solely responsible for the quality, timeliness and other terms and conditions of such maintenance services. Xerox shall have no liability for the acts or omissions of such third party service provider.

15. **COMMENCEMENT & TERM.** This Agreement is valid when accepted by Xerox. The term for a lease Order shall commence upon acceptance of the Equipment; provided, however, for "Customer-installable" Equipment, the term for a lease Order shall commence upon delivery of the Equipment. Unless a lease order is preceded by a trial order, the equipment will be considered accepted upon installation of the equipment by Lessor, after the equipment successfully runs all required diagnostic routines, and the equipment is turned over to the University for use.
16. **PAYMENT.** Payment must be received by Xerox within 30 days after the invoice date. All invoice payments under this Agreement shall be made via check, Automated Clearing House debit, Electronic Funds Transfer, or direct debit from University's bank account. Restrictive covenants on payment instruments will not reduce your obligations.
17. **SEPARATELY BILLED MAINTENANCE.** If a Minimum Payment is included in Maintenance Plan Features for an item of Equipment, the Minimum Payment for Maintenance Services will be billed separately.
18. **PRICE INCREASES.** Once a University enters into a lease agreement, the rate must remain fixed throughout the Initial Lease Term.
19. **DELIVERY, REMOVAL & RELOCATION.** Equipment prices include standard delivery charges and, for Xerox-owned Equipment, standard removal charges. Charges for non-standard delivery, excessive installation requirements, including rigging, access alterations, and access to non-ground floors via stairs. Any such excessive installation charges must be quoted to the University prior to the signature of any Order, and shall be based on the actual expenditures of Vendor or Authorized Dealer and for any Equipment relocation are the University's responsibility. Relocation of Xerox-owned Equipment must be arranged (or approved in advance) by Xerox and may not be to a location outside of the U.S.
20. **DEFAULT & REMEDIES.**

The University will be in default under this Agreement if (1) Xerox does not receive any payment within 15 days after the date it is due (45 days after date of invoice), or (2) you breach any other obligation in this or any other agreement with Xerox. If you default, Xerox may, in addition to its other remedies (including cessation of Maintenance Services), remove the Equipment and Third Party Hardware at your expense and require immediate payment, as liquidated damages for loss of bargain and not as a penalty of: (a) all amounts then due, plus interest from the due date until paid as allowed under California law; (b) the Minimum Lease Payments (less the Maintenance Services and Consumable Supplies components thereof, as reflected on Xerox's books and records) remaining in the Equipment Order Term, discounted at 4% per annum; and (c) the applicable fair market value
21. **TRADE-IN EQUIPMENT.** The University warrants that it has the right to transfer title to the equipment you are trading in as part of this Agreement ("Trade-In Equipment") and that the Trade-In Equipment is in good working order and has not been modified from its original configuration (other than by Xerox). Title and risk of loss to the Trade-In Equipment will pass to Xerox when Xerox removes it from your premises. The University will maintain the Trade-In Equipment at its present site and in substantially its present condition until removed by Xerox. The University will pay all accrued charges for the Trade-In Equipment (up to and including payment of the final principal payment number) and all applicable maintenance, administrative, supply and finance charges until Xerox removes the Trade-In Equipment from your premises.
22. **NON-CANCELABLE AGREEMENT.** THIS AGREEMENT CANNOT BE CANCELED OR TERMINATED EXCEPT AS EXPRESSLY PROVIDED HEREIN. YOUR OBLIGATION TO MAKE ALL PAYMENTS, AND TO PAY ANY OTHER AMOUNTS DUE OR TO BECOME DUE, IS ABSOLUTE AND UNCONDITIONAL AND NOT SUBJECT TO DELAY, REDUCTION, SET-OFF, DEFENSE, COUNTERCLAIM OR RECOUPMENT FOR ANY REASON WHATSOEVER, IRRESPECTIVE OF XEROX'S PERFORMANCE OF ITS OBLIGATIONS HEREUNDER. ANY CLAIM AGAINST XEROX MAY BE ASSERTED IN A SEPARATE ACTION AND SOLELY AGAINST XEROX.
23. **WARRANTY DISCLAIMER.** XEROX DISCLAIMS THE IMPLIED WARRANTIES OF NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE AND, FOR THIRD PARTY PRODUCTS, THE IMPLIED WARRANTY OF MERCHANTABILITY. This Agreement is a "finance lease" under Article 2A of the Uniform Commercial Code and, except to the extent expressly provided herein, and as permitted by applicable law, you waive all of your rights and remedies as a lessee under Article 2A.
24. **TITLE & RISK OF LOSS AND INSURANCE.** Until you exercise your Purchase Option: (a) title to Equipment and Third Party Hardware will remain with Xerox; (b) Equipment and Third Party Hardware will remain personal property; (c) you will

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

not attach the Equipment or Third Party Hardware as a fixture to any real estate; (d) you will not pledge, sub-lease or part with possession of the Equipment or Third Party Hardware, or file or permit to be filed any lien against the Equipment or Third Party Hardware; and, (e) you will not make any permanent alterations to the Equipment or Third Party Hardware. For equipment installed by Lessor Risk of loss will pass to the University upon acceptance and for equipment designated as "Customer Installable," the equipment delivery date the University will keep the Products and Third Party Products insured against loss or damage and the policy will name Xerox as a loss payee.

ADDITIONAL SOFTWARE TERMS (SOME EQUIPMENT AND ACCESSORIES)

25. FREEFLOW LICENSE. The following terms apply to Xerox FreeFlow Print Server /DocuSP software included in Base Software ("FreeFlow Base Software") and/or Application Software identified as Xerox FreeFlow software (including, but not limited to, FreeFlow Makeready and FreeFlow Process Manager) (collectively, "FreeFlow Application Software"), and are additive to and supplement those found elsewhere in the Agreement. FreeFlow Base Software and FreeFlow Application Software are collectively referred to as "FreeFlow Software."

1. FreeFlow Software may include and/or incorporate font programs ("Font Programs") and other software provided by Adobe Systems Incorporated ("Adobe Software"). You may embed copies of the Font Programs into your electronic documents for the purpose of printing and viewing the document. You are responsible for ensuring that you have the right and are authorized by any necessary third parties to embed any Font Programs in electronic documents created with the FreeFlow Application Software. If the Font Programs are identified as "licensed for editable embedding" at www.adobe.com/type/browser/legal/embeddingeula, you may also embed copies of those Font Programs for the additional purpose of editing your electronic documents. No other embedding rights are implied or permitted under this license.

2. You will not, without the prior written consent of Xerox and its licensors: (a) alter the digital configuration of the FreeFlow Software, or solicit others to cause the same, so as to change the visual appearance of any of the FreeFlow Software output; (b) use the FreeFlow Software in any way that is not authorized by the Agreement; (c) use the embedded code within the FreeFlow Software outside of the Equipment on which it was installed or in a stand-alone, time-share or service bureau model; (d) disclose the results of any performance or benchmark tests of the FreeFlow Software; (e) use the FreeFlow Software for any purpose other than to carry out the purposes of the Agreement; or (f) disclose or otherwise permit any other person or entity access to the object code of the FreeFlow Software.

3. FreeFlow Process Manager contains Oracle Database Express Edition database software and documentation licensed from Oracle America, Inc. ("Oracle"). Oracle grants you a nonexclusive, nontransferable limited license to use Database Express Edition for purposes of developing, prototyping and running your applications for your own internal data processing operations. Database Express Edition may be installed on a multiple CPU server but may only be executed on one processor in any server. Upon not less than 45 days prior written notice, Xerox and/or its licensors may, at their expense, directly or through an independent auditor, audit your use of FreeFlow Process Manager and all relevant records not more than once annually. Any such audit will be conducted at a mutually agreed location and will not unreasonably interfere with your business activities.

4. The Copyright Management feature of FreeFlow Makeready ("FFCM") contains the optional Copyright Clearance Center, Inc. ("CCC") copyright licensing services feature of FFCM ("CCC Service"). If this option is ordered, you will comply with any applicable terms and conditions contained on the CCC website, www.copyright.com, and any other rights holder terms governing use of materials, which are accessible in FFCM. If CCC terminates Xerox's right to offer access to the CCC Service through FFCM, Xerox may, upon written notice and without any liability to you, terminate your right to access the CCC Service through FFCM. THE CCC SERVICE IS PROVIDED "AS IS," WITHOUT ANY WARRANTIES, WHETHER EXPRESS OR IMPLIED. XEROX DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. You will defend and indemnify Xerox from any and all losses, claims, damages, fines, penalties, interest, costs and expenses, including reasonable attorney fees, arising from or relating to your use of the CCC Service. 5. If you install FreeFlow Application Software on a computer that you supply, the following terms apply: (a) Xerox will only be obligated to support FreeFlow Application Software if it is installed on hardware and software meeting Xerox's published specifications (collectively "Workstation"); (b) IF YOU USE FREEFLOW APPLICATION SOFTWARE WITH ANY HARDWARE OR SOFTWARE OTHER THAN A

WORKSTATION, ALL REPRESENTATIONS AND WARRANTIES ACCOMPANYING SUCH FREEFLOW APPLICATION SOFTWARE WILL BE VOID AND ANY SUPPORT/MAINTENANCE YOU CONTRACT FOR IN CONNECTION WITH SUCH FREEFLOW APPLICATION SOFTWARE WILL BE VOIDABLE AND/OR SUBJECT TO ADDITIONAL CHARGES; and (c) you are solely responsible for: (i) the acquisition and support, including any and all associated costs, charges and other fees, of any

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

Workstation you supply; (ii) compliance with all terms governing such Workstation acquisition and support, including terms applicable to any non-Xerox software associated with such Workstation; and (iii) ensuring that such Workstation meets Xerox's published specifications.

6. The following terms apply to FreeFlow Software licensed to U.S. government customers:

a. Java technology contained in FreeFlow Software is subject to: (i) FAR 52.227- 14(g)(2) and FAR 52.227-19; and (ii) if licensed to the U.S. Department of Defense ("DOD"), DFARS 252.227-7015(b) and DFARS 227.7202-3(a).

b. Adobe Software is a "commercial item," as that term is defined at FAR 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212, and is licensed to civilian agencies consistent with the policy set forth in FAR 12.212, or to the DOD consistent with the policies set forth in DFARS 227.7202-1.

c. Oracle Database Express Edition is "commercial computer software" and is subject to the restrictions as set forth in the Rights in Technical Data and Computer Software Clauses in DFARS 252.227-7015 and FAR 52.227-19 as applicable.

7. FreeFlow Software may include Microsoft Embedded Standard operating system software to which the following terms apply:

a. You agree to and will comply with the Microsoft terms and conditions contained on the Xerox website, <http://www.support.xerox.com/support/open-source-disclosures/filteredirect/enus.html?&contentId=136023>.

b. Any updates, upgrades or reinstallations of Microsoft Embedded Standard operating system software are subject to the terms and conditions of this license and may be used only with the Xerox-brand Equipment with which it was delivered. Any other use of the software is strictly prohibited and may subject you to legal action. c. If the Equipment includes Remote Desktop Services that enable it to connect to and access applications running on a server, such as Remote Desktop Protocol, Remote

Assistance and Independent Computer Architecture, such Desktop Functions will not run locally on the system, except for network/Internet browsing functions.

d. The FreeFlow Base Software contains the Windows Update feature that allows you to access Windows Updates directly through the Microsoft Corp. Windows Update server. If you elect to activate this feature, any Windows Updates installed by you using the Windows Update feature may not function on the Equipment or may cause malfunctions or cause harm to the Equipment. Before you download a Windows Update using this feature, you should contact Xerox so that Xerox can ensure that each

Windows Update is suitable for use on the Equipment and provide any necessary technical support for the installation and use of such Windows Update.

e. No High Risk Use. WARNING: The Windows Embedded 7 Standard operating system is not fault-tolerant. The Windows Embedded 7 Standard operating system is not designed or intended for

any use in any computing device where failure or fault of any kind of the Windows Embedded 7 Standard operating system could reasonably be seen to lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High Risk Use"). Xerox is not licensed to use, distribute, or sublicense the use of the Windows Embedded 7 Standard operating system in High Risk Use. High Risk Use is STRICTLY PROHIBITED.

Versant Products Extra Long Prints Terms

26. EXTRA LONG PRINTS. The following Equipment model(s), V180P may now, or in the future, have extra-long print capability, which is the ability to produce a print that is longer than 491mm. Maximum print length may vary by model. The meters for Equipment with extra-long print capability will register the following, as applicable: (i) for impressions greater than 491mm, up to and including 661mm, the Extra Long Impressions meter will register two (2) prints for each such extra-long print, in addition to registering one (1) print on either the Color Impressions meter (in the case of a color print) or the Black Impressions meter (in the case of a B&W print); (ii) for impressions greater than 661mm, up to and including 877mm, the Extra Long Impressions meter will register three (3) prints for each such extra-long print, in addition to registering one (1) print on either the Color Impressions meter (in the case of a color print) or the Black Impression meter (in the case of a B&W print); (iii) for impressions greater than 877mm, up to and including 1,083mm, the Extra Long Impressions meter will register four (4) prints for each such extra-long print, in addition to registering one (1) print on either the Color Impressions meter (in the case of a color print) or the Black Impression meter (in the case of a B&W print); and (iv) for impressions greater than 1,083mm, up to and including 1,299mm, the Extra Long Impressions meter will register five (5) prints for each such extra-long print, in addition to registering one (1) print on either the Color Impressions meter (in the case of a color print) or the Black Impression meter (in the case of a B&W print).

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

PURCHASE AND MAINTENANCE TERMS

27. Cash Purchase.

- A. **Title and Risk.** Title and risk of loss to Equipment will pass to Customer upon delivery and installation of the Equipment. Until the products are paid for in full Customer will insure the Product against loss or damage, and the policy will name Xerox as a loss payee.
- B. **Payment.** Customer's payment under a Cash Purchase Order shall consist of the Net Price amount for the Equipment purchased there under and all applicable Taxes.
- C. **Customer Default & Remedies.** If Customer defaults under the Contract or a Cash Purchase Order, Xerox, in addition to its other remedies (including the cessation of Maintenance Services if applicable), may require immediate payment of all amounts then due (including all applicable Taxes), plus interest on all amounts due from the due date until paid as allowed under California law.

28 MAINTENANCE SERVICES CUSTOMER OWNED EQUIPMENT. Except for Equipment and/or Third Party Hardware identified as "No Svc.", Xerox (or a designated servicer) will keep the Equipment and/or Third Party Hardware in good working order ("Maintenance Services"). The provision of Maintenance Services is contingent upon Customer facilitating timely and efficient resolution of Equipment and/or Third Party Hardware issues by: (a) utilizing Customer-implemented remedies provided by Xerox; (b) replacing Cartridges; and (c) providing information to and implementing recommendations provided by Xerox telephone support personnel. If an Equipment and/or Third Party Hardware issue is not resolved after completion of (a) through (c) above, Xerox will provide on-site support as provided herein. Maintenance Services will be provided during Xerox's standard working hours in areas open for repair service for the Equipment and/or Third Party Hardware. Maintenance Services excludes repairs due to: (i) misuse, neglect or abuse; (ii) failure of the installation site or the PC or workstation used with the Equipment and/or Third Party Hardware to comply with Xerox's published specifications or Third Party Hardware vendor's published specifications, as applicable; (iii) use of options, accessories or products not serviced by Xerox; (iv) non-Xerox alterations, relocation, service or supplies; or (v) failure to perform operator maintenance procedures identified in operator manuals. Replacement parts may be new, reprocessed or recovered and all replaced parts become Xerox's property. Xerox will, as your exclusive remedy for Xerox's failure to provide Maintenance Services, replace the Equipment with an identical model or, at Xerox's option, another model with comparable features and capabilities. There will be no additional charge for the replacement Equipment during the remainder of the initial Term. If meter reads are a component of your Equipment's Maintenance Plan, you will provide them using the method and frequency identified by Xerox. If you do not provide a meter reading for Equipment not capable of Remote Data Access, or if Remote Data Access is interrupted, Xerox may estimate the reading and bill you accordingly. For Third Party Hardware identified as "No Svc.", you may enter into a maintenance agreement with the Third Party Hardware vendor or its maintenance service provider, who shall be solely responsible for the quality, timeliness and other terms and conditions of such maintenance services. Xerox shall have no liability for the acts or omissions of such Third party service provider.

29. DEFAULT & REMEDIES. You will be in default under this Agreement if (1) Xerox does not receive any payment within 15 days after the date it is due (45 days after date of invoice), or (2) you breach any other obligation in this or any other agreement with Xerox.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

ADDITIONAL TERMS

These additional terms are incorporated into the Xerox Proposal and are in addition to the terms included in the University's RFP. Should there be a conflict between the various provisions the order of precedence shall be these Additional Terms followed by the University's RFP.

ADDITIONAL TERMS APPLICABLE TO ALL NON-UNIVERSITY ENTITIES

The following additional terms are incorporated into the Xerox Proposal and are in addition to the terms included in the University's RFP. Should there be a conflict between these Additional Terms and the terms of the University Contract, the OMNIA Partners Terms and Conditions will control followed by the University terms and conditions. Please note only relevant terms of the OMNIA Master Agreement applicable to Non-University entities are included in this section.

The terms of the OMNIA Master Agreement, which are incorporated to this Contract by their reference, will apply to Non-University entities to procure equipment and services under this Agreement. Xerox agrees to make resulting OMNIA Partners' pricing/terms from this solicitation available to other public agencies nationally, including state and local governmental entities, public and private primary, secondary and higher education entities, non-profit entities, and agencies for the public benefit ("Public Agencies") through OMNIA Partners' Cooperative purchasing program so long as such Public Agency is a registered member at OMNIA. OMNIA Partners Terms and Conditions - <https://www.sourcewell-mn.gov/cooperative-purchasing/083116-xox?domain=870%20%20%20%20%20%20%20%20%D0%B5H#tab-contract-documents>

General Terms and Conditions

1. **SCOPE.** The acquisition of Products and Maintenance Services by Customer is subject to the terms and conditions of the Region 4 ESC Contract R and the following terms and conditions (the "Agreement"). In the event of a conflict among these documents, the Region 4 Contract will take precedence. "Products" means Xerox-brand equipment ("Equipment"), Software and Consumable Supplies ordered under this Agreement.
2. **TERM.** The initial term of this Agreement ("Initial Term") will commence on the date it is accepted by Xerox, and it will expire on the last day of the 36th full calendar month thereafter, unless early terminated by either party upon not less than 90-days' notice. Following the Initial Term, this Agreement may be renewed for two (2) additional one-year terms, under the same terms and conditions. Upon the expiration or termination of this Agreement, each IA (as defined in Section 3.a.) shall remain in full force and effect until the end of its term and shall be governed by the terms and conditions of this Agreement as if it were still in effect.
3. **ORDER DOCUMENTS.**
 - a. Customer will issue documents that Customer or Xerox require for acquisitions hereunder, including purchase orders and individual standard form Xerox agreements ("Order Document(s)") for order entry purposes only, specifying Customer's requested shipment date, installation site, quantities, bill-to address and product description, including any Trade-In Equipment. Notwithstanding anything contained in any Order Document which is at variance with or additional to this Agreement, Order Documents will incorporate and be subject solely to the terms and conditions of this Agreement, except for standard Xerox agreement terms and conditions related to options selected by Customer at time of order. Xerox reserves the right to review and approve Customer's credit prior to acceptance of an Order Document, and Customer authorizes Xerox or its agent to obtain credit reports from commercial credit reporting agencies. Upon acceptance by Xerox, the Order Document creates an individual agreement ("IA") for the Products identified therein. An IA for "Standard Lease" or "Major Account Lease" may be referred to herein as a "Lease IA". An IA for "Cash Purchase" or "Major Account Purchase" may be referred to herein as a "Purchase IA".
 - b. Order Documents may be submitted by hard copy or electronic means and those submitted electronically will be considered: (i) a "writing" or "in writing"; (ii) "signed" by Customer; (iii) an "original" when printed from electronic records established and maintained in the ordinary course of business; and, (iv) valid and enforceable.
4. **ELIGIBLE AFFILIATES.** Xerox will provide Products under this Agreement to Customer's Members. If a Member submits an Order Document, it will be the "Customer" for purposes of the resulting IA. If Customer divests a Member, such divested entity is no longer eligible to submit Orders under this Agreement.
5. **PRODUCTS.** Customer represents that the Products: (i) will be used in Customer's business in the United States, its territories and possessions ("U.S."); (ii) are not being acquired for resale; and (iii) will not be used for personal, household

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

or family purposes. Xerox may, for purposes of future order-taking, add Products to this Agreement or withdraw Products that become no longer generally commercially available.

6. **EQUIPMENT STATUS.** Except for Equipment identified in an IA as "Previously Installed", Equipment will be (a) "Newly Manufactured", which may contain some reconditioned components; (b) "Factory Produced New Model", which is manufactured and newly serialized at a Xerox factory, adds functions and features to a product previously disassembled to a Xerox predetermined standard, and contains new and reconditioned components; or (c) "Remanufactured", which has been factory produced following disassembly to a Xerox predetermined standard and contains new and reconditioned components.
7. **EQUIPMENT COMMENCEMENT & INSTALLATION DATES.** The initial Term of an IA that includes Equipment will commence on the "Installation Date", which means: (a) for Equipment installed by Xerox, the date Xerox determines the Equipment to be operating satisfactorily and is available for Customer's use, as demonstrated by successful completion of diagnostic routines; and (b) for Equipment designated as "Customer Installable", the Equipment delivery date.
8. **DATA SECURITY.** Certain models of Equipment can be configured to include a variety of data security features. There may be an additional cost associated with certain data security features. The selection, suitability and use of data security features are solely Customer's responsibility. Upon request, Xerox will provide additional information to Customer regarding the security features available for particular Equipment models.
9. **MAINTENANCE SERVICES.** Except for Equipment identified as "No Svc.", Xerox (or a designated servicer) will keep the Equipment in good working order ("Maintenance Services"). The provision of Maintenance Services is contingent upon Customer facilitating timely and efficient resolution of Equipment issues by: (a) utilizing Customer-implemented remedies provided by Xerox; (b) replacing Cartridges; and (c) providing information to and implementing recommendations provided by Xerox telephone support personnel. If an Equipment issue is not resolved after completion of (a) through (c) above, Xerox will provide on-site support as provided in the applicable IA. Maintenance Services are provided as a mandatory part of a Lease or Rental IA, or under a Maintenance IA. Maintenance Services will be provided during Xerox's standard working hours in areas open for repair service for the Equipment. Maintenance Services excludes repairs due to: (a) misuse, neglect or abuse; (b) failure of the installation site or the PC or workstation used with the Equipment to comply with Xerox's published specifications; (c) use of options, accessories or products not serviced by Xerox; (d) non-Xerox alterations, relocation, service or supplies; or (e) failure to perform operator maintenance procedures identified in operator manuals. Replacement parts may be new, reprocessed or recovered and all replaced parts become Xerox's property. If Xerox is unable to repair the Equipment so that it performs consistently in accordance with its specifications, Xerox will replace the Equipment with an identical model or, at Xerox's option, another model with comparable features and capabilities. There will be no additional charge for the replacement Equipment during the remainder of the initial Term. If meter reads are a component of a Maintenance Plan, Customer will provide them using the method and frequency identified by Xerox. If Customer does not provide a meter reading for Equipment not capable of Remote Data Access, or if Remote Data Access is interrupted, Xerox may reasonably estimate the reading and bill Customer accordingly.
10. **CARTRIDGES.** If Xerox is providing Maintenance Services for Equipment utilizing cartridges designated by Xerox as customer-replaceable units, including copy/print cartridges and xerographic modules or fuser modules ("Cartridges"), Customer agrees to use only unmodified Cartridges purchased directly from Xerox or its authorized resellers in the United States and the failure to use such Cartridges shall void any warranty applicable to such Equipment. Cartridges packed with Equipment and replacement Cartridges may be new, remanufactured, or reprocessed. Remanufactured and reprocessed Cartridges meet Xerox's new Cartridge performance standards and contain new and/or reprocessed components. To enhance print quality, Cartridge(s) for many models of Equipment have been designed to cease functioning at a predetermined point. In addition, many Equipment models are designed to function only with Cartridges that are newly manufactured original Xerox Cartridges or with Cartridges intended for use in the U.S. Equipment configuration that permits use of non-newly manufactured original Xerox Cartridges may be available from Xerox at an additional charge.
11. **DELIVERY & REMOVAL.** Equipment prices include standard delivery charges for all Equipment and, for Equipment for which Xerox retains ownership, standard removal charges. Non-standard delivery or removal will be at Customer's expense.
12. **PAYMENT & TAXES.**
 - a. If the invoice displays a due date, payment must be received by Xerox on or before the due date. If the invoice does not display a due date, payment must be received by Xerox in accordance with the state's prompt payment statutes, or, if such statutes are not applicable, within 30 days after the invoice date. All invoice payments under this Agreement shall be made via check, Automated Clearing House debit, Electronic Funds Transfer, or direct debit from Customer's bank account. Restrictive covenants on payment instruments will not reduce Customer's obligations.
 - b. Customer is responsible for all applicable taxes, fees or charges of any kind (including interest and penalties) assessed by any governmental entity on this Agreement or the amounts payable under this Agreement ("Taxes"), which will be

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

included in Xerox's invoice unless Customer timely provides proof of its tax exempt status. Taxes do not include taxes on Xerox's income and, for Lease IAs, Taxes do not include personal property taxes in jurisdictions where Xerox is required to pay personal property taxes. Except for Equipment that includes a Bargain Purchase Option, a Lease IA is a lease for all income tax purposes and Customer will not claim any credit or deduction for depreciation of the Equipment or take any other action inconsistent with its role as lessee of the Equipment.

- 13. LATE CHARGES & DEFAULT.** If a payment is not received by Xerox within 10 days after the due date, Xerox may charge, and Customer will pay, a late charge equal to 5% of the amount due or \$25, whichever is greater, or the amount allowed by applicable law, if less. Customer will be in default under an IA if Xerox does not receive any payment within 15 days after the date it is due or Customer breaches any other obligation under this Agreement, any IA hereunder, or any other agreement with Xerox. Customer will pay all reasonable costs, including attorneys' fees, incurred by Xerox to enforce this Agreement or any IA.
- 14. NON-CANCELABLE AGREEMENT.** LEASE AND INSTALLMENT PURCHASE IA's CANNOT BE CANCELED OR TERMINATED EXCEPT AS EXPRESSLY PROVIDED HEREIN. CUSTOMER'S OBLIGATION TO MAKE ALL PAYMENTS, AND TO PAY ANY OTHER AMOUNTS DUE OR TO BECOME DUE, IS ABSOLUTE AND UNCONDITIONAL AND NOT SUBJECT TO DELAY, REDUCTION, SET-OFF, DEFENSE, COUNTERCLAIM OR RECOUPMENT FOR ANY REASON WHATSOEVER, IRRESPECTIVE OF XEROX'S PERFORMANCE OF ITS OBLIGATIONS HEREUNDER. ANY CLAIM AGAINST XEROX MAY BE ASSERTED IN A SEPARATE ACTION AND SOLELY AGAINST XEROX.
- 15. WARRANTY DISCLAIMER & WAIVERS.** XEROX DISCLAIMS THE IMPLIED WARRANTIES OF NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.
- 16. LEASE OPTIONS FOR PURCHASE, RENEWAL, AND TERMINATION.** The following options are available for Equipment under a Lease IA:
 - a. If not in default hereunder, Customer may purchase the Equipment, "AS IS, WHERE-IS" and WITHOUT ANY WARRANTY AS TO CONDITION OR VALUE, at the end of the initial Term of a Lease IA for the purchase option indicated in such IA, plus all applicable Taxes.
 - b. Unless either party provides notice of termination at least 30 days before the end of the initial Term of a Lease IA, it will renew automatically on a month-to-month basis on the same terms and conditions. During this renewal period, either party may terminate the Lease IA upon at least 30 days' notice. Upon termination, Customer will make the Equipment available for removal by Xerox. At the time of removal, the Equipment will be in the same condition as when delivered (reasonable wear and tear excepted).
- 17. INTELLECTUAL PROPERTY INDEMNITY.** Xerox will defend, and pay any settlement agreed to by Xerox or any final judgment for, any claim that a Xerox-brand Product infringes a third party's U.S. intellectual property rights. Customer will promptly notify Xerox of any alleged infringement and permit Xerox to direct the defense. Xerox is not responsible for any non-Xerox litigation expenses or settlements unless Xerox pre-approves them in writing. To avoid infringement, Xerox may modify or substitute an equivalent Xerox-brand Product and, if purchased, refund the price paid for the Xerox-brand Product (less the reasonable rental value for the period it was available to Customer), or obtain any necessary licenses. Xerox is not liable for any infringement based upon a Xerox-brand Product being modified to Customer's specifications or being used or sold with products not provided by Xerox.
- 18. LIMITATION OF LIABILITY.** For claims arising out of or relating to this Agreement or any IA written hereunder, whether the claim alleges tortious conduct (including negligence) or any other legal theory, but excepting liability under the indemnification obligations set forth in this Agreement, Xerox will not be liable to Customer for any direct damages relating to this Agreement or any IA written hereunder in excess of the sum of the amounts paid and to be paid during the initial Term of the applicable IA and neither party will be liable to the other for any special, indirect, incidental, consequential or punitive damages.
- 19. ASSIGNMENT.** Neither party may assign without the prior written consent of the other party.
- 20. NOTICES.** Unless provided otherwise in this Agreement, notices under this Agreement or any IA must be sent in writing to the party's address or facsimile number set forth below. Notices will be deemed given 5 days after mailing by first class mail, 2 days after sending by nationally recognized overnight courier, or on the date of electronic confirmation of receipt of a facsimile transmission, when followed by mailing of such notice as provided herein. Invoices are not considered notices under this Agreement and are governed by provisions relating specifically thereto. All payment related notices under an IA shall be sent: (a) to Customer at the "Bill to" address in the IA, and (b) to Xerox at the inquiry address on the most recent invoice. All other notices under this Agreement or an IA shall be sent to a party at its address or facsimile number below. Either party may change its address or facsimile number for receipt of notice by notifying the other party at its address or facsimile number below.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

To Customer:

To Xerox:

**Office of General Counsel
Xerox Corporation
45 Glover Avenue
P. O. Box 4505
Norwalk, CT 06856-4505**

Facsimile:

Facsimile:

- 21. FORCE MAJEURE.** Xerox will not be liable to Customer during any period in which its performance is delayed or prevented, in whole or in part, by a circumstance beyond its reasonable control. Xerox will notify Customer if such a circumstance occurs.
- 22. CONSUMABLE SUPPLIES.** Consumable Supplies vary depending upon the Equipment model. If "Consumable Supplies" is identified in Maintenance Plan Features, Consumable Supplies include: (i) for black and white Equipment, standard black toner and/or dry ink, black developer, Copy Cartridges, and, if applicable, fuser agent required to make impressions; (ii) for full color Equipment, the items in (i) plus standard cyan, magenta, and yellow toners and dry inks (and their associated developers); and, (iii) for Equipment identified as "Phaser", only, if applicable, black solid ink, color solid ink, imaging units, waste cartridges, transfer rolls, transfer belts, transfer units, belt cleaner, maintenance kits, print Cartridges, drum Cartridges, waste trays and cleaning kits. Xerox may charge a shipping and handling fee for Consumable Supplies. Consumable Supplies are Xerox's property until used by Customer, and Customer will use them only with the Equipment for which "Consumable Supplies" is identified in Maintenance Plan Features. If Consumables Supplies are furnished with recycling information, Customer will return the used item, at Xerox's expense, for remanufacturing. Shipping information is available at Xerox.com/GWA. Upon expiration of this Agreement, Customer will include any unused Consumable Supplies with the Equipment for return to Xerox at the time of removal. If Customer's use of Consumable Supplies exceeds Xerox's published yield by more than 10%, Xerox will notify Customer of such excess usage. If such excess usage does not cease within 30 days after such notice, Xerox may charge Customer for such excess usage. Upon request, Customer will provide current meter reads and/or an inventory of Consumable Supplies in its possession.
- 23. RELOCATION.** Until Customer has paid in full under a Purchase IA or Installment Purchase IA, or while Equipment is subject to a Lease or Rental IA: (a) all Equipment relocations must be arranged (or approved in advance) by Xerox and will be at Customer's expense; (b) while Equipment is being relocated, Customer remains responsible to make all payments under the applicable IA; and (c) Equipment cannot be relocated outside of the U.S.
- 24. SOFTWARE**
- a. **SOFTWARE LICENSE.** Xerox grants Customer a non-exclusive, non-transferable license to use in the U.S.: (a) software and accompanying documentation provided with Xerox-brand Equipment ("Base Software") only with the Xerox-brand Equipment with which it was delivered; and (b) software and accompanying documentation identified in an IA as "Application Software" only on any single unit of equipment for as long as Customer is current in the payment of all applicable software license fees. "Base Software" and "Application Software" are referred to collectively as "Software". Customer has no other rights and may not: (1) distribute, copy, modify, create derivatives of, decompile, or reverse engineer Software; (2) activate Software delivered with the Equipment in an inactivated state; or (3) allow others to engage in same. Title to, and all intellectual property rights in, Software will reside solely with Xerox and/or its licensors (who will be considered third-party beneficiaries of this subsection a.). Software may contain code capable of automatically disabling the Equipment. Disabling code may be activated if: (x) Xerox is denied access to periodically reset such code; (y) Customer is notified of a default under an IA; or (z) Customer's license is terminated or expires. The Base Software license will terminate: (i) if Customer no longer uses or possesses the Equipment; (ii) Customer is a lessor of the Equipment and its first lessee no longer uses or possesses it; or (iii) upon the expiration of any IA under which Customer has rented or leased the Equipment (unless Customer has exercised an option to purchase the Equipment). Neither Xerox nor its licensors warrant that Software will be free from errors or that its operation will be uninterrupted. The foregoing terms do not apply to Diagnostic Software or to software/documentation accompanied by a clickwrap or shrinkwrap license agreement or otherwise made subject to a separate license agreement.
- b. **SOFTWARE SUPPORT.** Xerox (or a designated servicer) will provide the software support set forth below ("Software Support"). For Base Software, Software Support will be provided during the initial Term of the applicable IA and any renewal period but in no event longer than 5 years after Xerox stops taking customer orders for the subject model of Equipment. For Application Software, Software Support will be provided as long as Customer is current in the payment of all applicable software license and support fees. Xerox will maintain a web-based or toll-free hotline during Xerox's standard working hours to report Software problems and answer Software-related questions. Xerox, either directly or with its vendors, will make reasonable efforts to: (a) assure that Software performs in material conformity with its user

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

documentation; (b) provide available workarounds or patches to resolve Software performance problems; and (c) resolve coding errors for (i) the current Release and (ii) the previous Release for a period of 6 months after the current Release is made available to Customer. Xerox will not be required to provide Software Support if Customer has modified the Software. New releases of Software that primarily incorporate compliance updates and coding error fixes are designated as "Maintenance Releases" or "Updates". Maintenance Releases or Updates that Xerox may make available will be provided at no charge and must be implemented within 6 months. New releases of Software that include new content or functionality ("Feature Releases") will be subject to additional license fees at Xerox's then-current pricing. Maintenance Releases, Updates, and Feature Releases are collectively referred to as "Releases". Each Release will be considered Software governed by the SOFTWARE LICENSE and SOFTWARE SUPPORT provisions of this Agreement (unless otherwise noted). Implementation of a Release may require Customer to procure, at Customer's expense, additional hardware and/or software from Xerox or another entity. Upon installation of a Release, Customer will return or destroy all prior Releases. Xerox may annually increase the Annual Renewal and Support-Only Fees for Application Software. For State and Local Government Customers, this adjustment will take place at the commencement of each of Customer's annual contract cycles.

- c. **DIAGNOSTIC SOFTWARE.** Software used to evaluate or maintain the Equipment ("Diagnostic Software") is included with the Equipment. Diagnostic Software is a valuable trade secret of Xerox. Title to Diagnostic Software will remain with Xerox or its licensors. Xerox does not grant Customer any right to use Diagnostic Software, and Customer will not access, use, reproduce, distribute or disclose Diagnostic Software for any purpose (or allow third parties to do so). Customer will allow Xerox reasonable access to the Equipment to remove or disable Diagnostic Software if Customer is no longer receiving Maintenance Services from Xerox, provided that any on-site access to Customer's facility will be during Customer's normal business hours.

25. REMOTE SERVICES.

- a. Certain models of Equipment are supported and serviced using data that is automatically collected by Xerox or transmitted to or from Xerox by Equipment connected to Customer's network ("Remote Data") via electronic transmission to a secure off-site location ("Remote Data Access"). Remote Data Access also enables Xerox to transmit to Customer Releases for Software and to remotely diagnose and modify Equipment to repair and correct malfunctions. Examples of Remote Data include product registration, meter read, supply level, Equipment configuration and settings, software version, and problem/fault code data. Remote Data may be used by Xerox for billing, report generation, supplies replenishment, support services, recommending additional products and services, and product improvement/development purposes. Remote Data will be transmitted to and from Customer in a secure manner specified by Xerox. Remote Data Access will not allow Xerox to read, view or download the content of any Customer documents or other information residing on or passing through the Equipment or Customer's information management systems. Customer grants the right to Xerox, without charge, to conduct Remote Data Access for the purposes described above.
- b. Upon Xerox's request, Customer will provide contact information for Equipment such as name and address of Customer contact and IP and physical addresses/locations of Equipment. Customer will enable Remote Data Access via a method prescribed by Xerox, and Customer will provide reasonable assistance to allow Xerox to provide Remote Data Access. Unless Xerox deems Equipment incapable of Remote Data Access, Customer will ensure that Remote Data Access is maintained at all times Maintenance Services are being performed.

- 26. TRADE-IN EQUIPMENT.** Customer warrants that Customer has the right to transfer title to the equipment Customer is trading in as part of an IA ("Trade-In Equipment"), and that the Trade-In Equipment is in good working order and has not been modified from its original configuration (other than by Xerox). Title and risk of loss to the Trade-In Equipment will pass to Xerox when Xerox removes it from Customer's premises. Customer will maintain the Trade-In Equipment at its present site and in substantially its present condition until removed by Xerox. Customer will pay all accrued charges for the Trade-In Equipment (up to and including payment of the final principal payment number) and all applicable maintenance, administrative, supply and finance charges until Xerox removes the Trade-In Equipment from Customer's premises.

27. TOTAL SATISFACTION GUARANTEE.

- a. "SP Equipment" means any iGen3, iGen4, iGen150, iGen5 or Xerox Color 8250 Production Printer. If, during any 90 day period, the performance of SP Equipment delivered under this Agreement is not at least substantially consistent with the performance expectations outlined in the SP Equipment's Customer Expectations Document ("Expectations Document"), Xerox will, at Customer's request, replace the SP Equipment without charge with identical SP Equipment or, at Xerox's option, with Equipment with comparable features and capabilities (the "SP Equipment Guarantee"). The SP Equipment Guarantee does not apply during the first 180 days after installation and will expire 3 years after the Installation Date, unless the SP Equipment is being financed under this Agreement for more than 3 years, in which event it expires at the end of the initial Term of the subject Installment Purchase, Rental or Lease IA; provided however, for SP Equipment identified as "Previously Installed", this SP Equipment Guarantee expires 1 year after installation.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

This SP Equipment Guarantee applies only to SP Equipment that has been (i) continuously maintained by Xerox under a Xerox maintenance agreement, and (ii) operated at all times in accordance with the Expectations Document.

- b. "Non-SP Equipment" means any Equipment other than SP Equipment. If Customer is not completely satisfied with any Non-SP Equipment delivered under an IA under this Agreement, Xerox will, at Customer's request, replace it without charge with identical Non-SP Equipment or, at the option of Xerox, with Equipment with comparable features and capabilities (the "Non-SP Equipment Guarantee"). The Non-SP Equipment Guarantee applies only to Non-SP Equipment that has been continuously maintained by Xerox under a Xerox maintenance agreement. The Non-SP Equipment Guarantee is effective for 3 years after the Installation Date, unless the Non-SP Equipment is being acquired under an Installment Purchase, Rental or Lease IA with an initial Term of more than 3 years, in which event it will expire at the end of the initial Term of the subject IA; provided however, for Non-SP Equipment identified as "Previously Installed", the Non-SP Equipment Guarantee expires 1 year after the Installation Date. The Non-SP Equipment Guarantee does not apply to a limited number of Non-SP Equipment models, which models are identified in the applicable Order Document.
- c. The SP Equipment Guarantee and Non-SP Equipment Guarantee replace and supersede any other guarantee from Xerox, whether made orally or in writing, styled a "Total Satisfaction Guarantee", "Satisfaction Guarantee" or otherwise covering the subject matter set forth above.

28. GOVERNMENT CUSTOMER TERMS: The following additional terms apply to Lease and Installment Purchase IA's:

- a. REPRESENTATIONS & WARRANTIES, FUNDING, TAX TREATMENT & PAYMENTS:
 - (i) REPRESENTATIONS & WARRANTIES. Customer represents and warrants, as of the date of this Agreement and of each IA hereunder, that: (1) Customer is a State or a fully constituted political subdivision or agency of the State in which Customer is located and is authorized to enter into, and carry out, Customer's obligations under this Agreement, any IA hereunder and any other documents required to be delivered in connection with the Agreement or any IA hereunder (collectively, the "Documents"); (2) the Documents have been duly authorized, executed and delivered by Customer in accordance with all applicable laws, rules, ordinances and regulations (including all applicable laws governing open meetings, public bidding and appropriations required in connection with this Agreement or an IA hereunder and the acquisition of the Products) and are valid, legal, binding agreements, enforceable in accordance with their terms; (3) the person(s) signing the Documents have the authority to do so, are acting with the full authorization of Customer's governing body and hold the offices indicated below their signatures, each of which are genuine; (4) the Products are essential to the immediate performance of a governmental or proprietary function by Customer within the scope of Customer's authority and will be used only by Customer and only to perform such function; (5) Customer's obligations to remit payments under this Agreement or any IA hereunder constitute a current expense and not a debt under applicable state law; and (6) no provision of this Agreement or any IA constitutes a pledge of Customer's tax or general revenues and any provision that is so construed by a court of competent jurisdiction is void from the inception of this Agreement or the subject IA.
 - (ii) FUNDING. Customer represents and warrants that all payments due and to become due during Customer's current fiscal year are within the fiscal budget of such year and are included within an unrestricted and unencumbered appropriation currently available for the lease/purchase of the Products, and it is Customer's intent to use the Products for the entire lease term and to make all payments required under this Agreement or an IA hereunder. If (1) through no action initiated by Customer, Customer's legislative body does not appropriate funds for the continuation of this Agreement or an IA hereunder for any fiscal year after the first fiscal year and has no funds to do so from other sources, and (2) Customer has made a reasonable but unsuccessful effort to find a creditworthy assignee acceptable to Xerox in its sole discretion within Customer's general organization who can continue this Agreement or an IA hereunder, this Agreement or an IA hereunder may be terminated. To effect this termination, Customer must, 30 days prior to the beginning of the fiscal year for which Customer's legislative body does not appropriate funds for such upcoming fiscal year, notify Xerox that Customer's legislative body failed to appropriate funds and that Customer has made the required effort to find an assignee. Customer's notice must be accompanied by payment of all sums then owed through the current year under this Agreement or any IA hereunder and must certify that canceled Equipment is not being replaced by equipment performing similar functions during the ensuing fiscal year. Customer will return the Equipment, at Customer's expense, to a location designated by Xerox and, when returned, the Equipment will be in good condition and free of all liens and encumbrances. Customer will then be released from any further payments obligations beyond those payments due for the current fiscal year (with Xerox retaining all sums paid to date).
 - (iii) TAX TREATMENT. Xerox has accepted this Agreement and each IA hereunder based on Customer's representation that Xerox may claim any interest paid by Customer as exempt from federal income tax under Section 103(c) of the Code. Customer will comply with the information reporting requirements of Section 149(e)

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

of the Code. Such compliance includes the execution of 8038-G or 8038-GC Information Returns. Customer appoints Xerox as Customer's agent to maintain, and Xerox will maintain, or cause to be maintained, a complete and accurate record of all assignments of this Agreement or an IA hereunder in form sufficient to comply with the book entry requirements of Section 149(a) of the Code and the regulations prescribed thereunder from time to time. Should Xerox lose the benefit of this exemption as a result of Customer's failure to comply with or be covered by Section 103(c) or its regulations, then, subject to the availability of funds and upon demand by Xerox, Customer will pay Xerox an amount equal to its loss in this regard. Customer will provide Xerox with a properly prepared and executed copy of US Treasury Form 8038 or 8038-GC.

(iv) **PAYMENTS.** All payments are due within 30 days of the invoice date.

27. AMENDMENT. All changes to this Agreement or any IA hereunder must be made in a writing signed by both parties. The amendment of this Agreement or any IA shall not affect the obligations of either party under any other IA's under this Agreement.

28. REPRESENTATIONS. The individuals signing this Agreement are duly authorized to do so and all financial information Customer provides completely and accurately represents Customer's financial condition.

29. MISCELLANEOUS. This Agreement is governed by the laws of the State of New York (without regard to conflict-of-law principles). In any action to enforce this Agreement or any IA hereunder, the parties agree (a) to the jurisdiction and venue of the federal and state courts (i) for Region 4 ESC, in Harris County, Texas, and (ii) for Members, in the specific jurisdiction and venue of the Member and (b) to waive their right to a jury trial. If a court finds any term of this Agreement or any IA unenforceable, the remaining terms will remain in effect. The failure by either party to exercise any right or remedy will not constitute a waiver of such right or remedy. Customer authorizes Xerox or its agents to communicate with Customer by any electronic means (including cellular phone, email, automatic dialing and recorded messages) using any phone number (including cellular) or electronic address Customer provides to Xerox. Each party may retain a reproduction (e.g., electronic image, photocopy, facsimile) of this Agreement and each IA hereunder which will be admissible in any action to enforce it, but only the Agreement or IA held by Xerox will be considered an original. Xerox may accept this Agreement or any IA hereunder either by signature or by commencing performance. Administrative and contract support functions hereunder may be performed, inside or outside the U.S., by one or more of Xerox's subsidiaries or affiliates and/or third parties. The following four sentences control over every other part of this Agreement and any IA hereunder. Both parties will comply with applicable laws. Xerox will not charge or collect any amounts in excess of those allowed by applicable law. Any part of this Agreement or any IA that would, but for the last four sentences of this Section, be read under any circumstances to allow for a charge higher than that allowed under any applicable legal limit, is modified by this Section to limit the amounts chargeable under this Agreement or any IA to the maximum amount allowed under the legal limit. If, in any circumstances, any amount in excess of that allowed by law is charged or received, any such charge will be deemed limited by the amount legally allowed and any amount received by Xerox in excess of that legally allowed will be applied by Xerox to the payment of amounts legally owed under this Agreement or the subject IA, or refunded to Customer.

30. ENTIRE AGREEMENT. The following are attached hereto and made part hereof:

- ARTICLE I: PURCHASE AND STANDARD LEASE TERMS AND CONDITIONS
- ARTICLE II: MAJOR ACCOUNT LEASE AND PURCHASE TERMS AND CONDITIONS
- ARTICLE III: RENTAL TERMS AND CONDITIONS
- ARTICLE IV: MAINTENANCE TERMS AND CONDITIONS
- ARTICLE V: MAJOR ACCOUNT MAINTENANCE TERMS AND CONDITIONS

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

ARTICLE II: MAJOR ACCOUNT LEASE TERMS AND CONDITIONS

Customer's acquisition of Equipment by Major Account Lease is governed by the terms and conditions of the Agreement and this Article.

1. **PRICING.** The Minimum Payment and Print Charges will not increase during the initial Term of a Major Account Lease IA.
2. **TERM.** The initial Term for any Major Account Lease IA will be the number of full calendar months stated in such IA. The Minimum Payment for any partial month following the Installation Date will be billed on a pro rata basis, based on a 30-day month.
3. **TITLE AND RISK.** Title to the Equipment remains with Xerox until Customer exercises its Purchase Option. Risk of loss or damage to the Products passes to Customer upon delivery. Customer will insure the Products against loss or damage and the policy will name Xerox as Loss Payee.
4. **PROTECTION OF XEROX'S RIGHTS.** Customer authorizes Xerox or its agent to file financing statements necessary to protect Xerox's rights as lessor of the Equipment. Until Customer has paid in full pursuant to the Purchase Option under a Major Account Lease IA, Equipment will remain personal property and Customer will not: (a) attach it as a fixture to any real estate; (b) pledge, sub-lease or part with possession of it; (c) file or permit to be filed any lien against it; or (d) make any permanent alterations to it. Customer will promptly notify Xerox if Customer relocates its principal place of business or changes the name of its business.
5. **REMEDIES.** If Customer defaults under the Agreement or any Major Account Lease IA, Xerox may, in addition to its other remedies (including cessation of Maintenance Services), remove the Equipment at Customer's expense and require immediate payment, as liquidated damages for loss of bargain and not as a penalty, of: (a) all amounts then due, plus interest from the due date until paid at the rate of 1.5% per month; (b) the Minimum Payments (less the Maintenance Services and Consumable Supplies components thereof, as reflected on Xerox's books and records) remaining in the initial Term of the Major Account Lease IA, discounted at 4% per annum; (c) the applicable Purchase Option; and (d) all applicable Taxes. You will pay all reasonable costs, including attorneys' fees, incurred by Xerox to enforce this Agreement. If Customer notifies Xerox and makes the Equipment available for removal by Xerox in the same condition as when delivered (reasonable wear and tear excepted) within 30 days after notice of default, Customer, upon recovery of the Equipment by Xerox, will receive a credit for the fair market value of the Equipment (as determined by Xerox), less any costs incurred by Xerox.
6. **FINANCE LEASE.** A MAJOR ACCOUNT LEASE IA IS A "FINANCE LEASE" UNDER ARTICLE 2A OF THE UNIFORM COMMERCIAL CODE AND, EXCEPT TO THE EXTENT EXPRESSLY PROVIDED HEREIN, AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, CUSTOMER WAIVES ALL RIGHTS AND REMEDIES CONFERRED UPON A LESSEE BY ARTICLE 2A.

END OF ARTICLE

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

ARTICLE IV : MAINTENANCE TERMS AND CONDITIONS

Customer's acquisition of Maintenance Services by a Maintenance IA or under a Lease or Rental IA is governed by the terms and conditions of the Agreement and this Article.

1. **MAINTENANCE TERM.** The initial Term of a Maintenance IA will commence: (a) for newly installed Equipment, on the Installation Date; (b) for all other Equipment, on the date Xerox accepts the Maintenance IA. The initial Term of a Maintenance IA will expire on the last day of the final calendar month of the initial Term, unless Customer chooses to renew the Maintenance IA for an equivalent term.
2. **INDIVIDUAL AGREEMENT PRICING.** Except as otherwise provided in a Maintenance IA, Xerox may annually increase the Minimum Payment and Print Charges under a Maintenance IA upon 30 days' notice.
3. **REMEDIES.** If Customer defaults under this Agreement or a Maintenance IA, Xerox, in addition to its other remedies (including the cessation of Maintenance Services), may require immediate payment, as liquidated damages for loss of bargain and not as a penalty, of: (a) all amounts then due, plus interest on all amounts due from the due date until paid at the rate of one and one-half percent (1.5%) per month (b) the lesser of (i) the remaining Minimum Payments in the initial term of the Maintenance IA, or (ii) six (6) such payments for one year agreements or twelve (12) such payments for multi-year agreements; and, (c) all applicable Taxes.
4. **RELOCATION.** If notified by Customer, Xerox will continue to provide Maintenance Services on Equipment relocated by Customer, provided that such relocation is to an area where Xerox offers Maintenance Services for the affected Equipment.

END OF ARTICLE

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

ADDITIONAL TERMS: SERVICES MASTER AGREEMENT

The following Service Master Agreement will be used by Non-University Customers when procuring managed print services, including maintenance services, Products (Software, Equipment, Third Party Products and/or Consumable Supplies supplied by Xerox and provided to Customer pursuant to an Order.

THIS SERVICES MASTER AGREEMENT NO. << Enter 7 Digit Contract Number >>> is between Xerox Corporation ("Xerox"), a New York corporation with offices at 45 Glover Ave. Norwalk, CT 06856 and << Enter Customer's Legal Name >>> ("Customer").

AGREEMENT STRUCTURE

This Agreement serves as a master agreement to enable Xerox and Customer to contract with each other for a range of products and services to be provided to the Customer over time. This Agreement is grouped into Modules. However, it is the intent of the parties that the Products and Services acquired hereunder be acquired under the auspices of the Region 4 ESC Contract # R171406 between Region 4 ESC and Xerox (the "Region 4 ESC Contract"). Therefore, the terms and conditions of the Region 4 ESC Contract are incorporated by reference into this Agreement. Any conflict between the terms and conditions of the Region 4 ESC Contract and this Agreement will be resolved in favor of this Agreement.

The "GEN" Module applies to all products and services provided hereunder, while the other Modules apply as appropriate to what Xerox is providing to Customer under the applicable Order.

DEFINITIONS MODULE

DEF 1. – DEFINITIONS

The following definitions (and those found elsewhere in this Agreement) apply unless otherwise specified in an Order.

- a. **Affiliate** means a legal entity that directly or indirectly controls, is controlled by, or is under common control with either party. An entity is considered to control another entity if it owns, directly or indirectly, more than 50% of the total voting securities or other such similar voting rights.
- b. **Agreement** means this Services Master Agreement. This Agreement may also be referred to in ordering and contracting documents as a "Services and Solutions Agreement" or "SSA."
- c. **Amortized Services** means certain services such as consulting and training, the Charges for which are amortized over the term of an Order.
- d. **Application Software** means Xerox-brand software that allows Equipment or Third Party Hardware to perform functions beyond those enabled by its Base Software.
- e. **Base Software** means software embedded, installed, or resident in Equipment that is necessary for operation of the Equipment in accordance with published specifications.
- f. **Cartridges** means copy/print cartridges and xerographic modules or fuser modules designated by Xerox as customer-replaceable units for the Equipment.
- g. **Charges** mean the fees payable by Customer for Services, Maintenance Services and/or Products as specified in this Agreement.
- h. **Confidential Information** means information identified as confidential and provided by the disclosing party to the receiving party.
- i. **Consumable Supplies.** Consumable Supplies vary depending upon the Equipment model, and include: (i) for black and white Equipment, standard black toner and/or dry ink, black developer, Copy Cartridges, and, if applicable, fuser agent required to make impressions; (ii) for full color Equipment, the items in (i) plus standard cyan, magenta, and yellow toners and dry inks (and their associated developers); and, (iii) for Equipment identified as "Phaser", only, if applicable, black solid ink, color solid ink, imaging units, waste cartridges, transfer rolls, transfer belts, transfer units, belt cleaner, maintenance kits, print Cartridges, drum Cartridges, waste trays and cleaning kits. Unless otherwise set forth in an Order, Consumable Supplies excludes paper and staples.
- j. **Customer Assets** means all hardware, equipment, fixtures, software, assets, networks, work space, facilities, services and other assets owned, leased, rented, licensed or controlled by Customer (including Existing Equipment

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

and Existing Software) that Customer makes available to Xerox to enable Xerox to fulfill its obligations under an Order.

- k. **Customer Confidential Information** means Confidential Information belonging to Customer and includes, without limitation, Customer Content and Private Information.
- l. **Customer Content** means documents, materials, or information that Customer provides in hard copy or electronic format to Xerox, containing information about Customer or its clients, in order for Xerox to provide Services, Maintenance Services, or Products.
- m. **Customer Facilities** means those facilities controlled by Customer where Xerox performs Services or provides Products.
- n. **Customer Intellectual Property** means all intellectual property and associated intellectual property rights including patent, trademark, service mark, copyright, trade dress, logo and trade secret rights which exist and belong to Customer as of the Effective Date or that may be created by Customer after the Effective Date, excluding Xerox Confidential Information.
- o. **Data** means data that the Xerox Tools and Xerox Client Tools automatically collect from all Equipment and Third Party Hardware that appears on Customer's network, or that are locally connected to another device on Customer's network, when such Tools are installed on Customer's network. Examples of Data include product registration, meter read, supply level, device configuration and settings, software version, and problem/fault code data.
- p. **Date of Installation** means: (a) for Equipment (or Third Party Hardware) installed by Xerox, the date Xerox determines the Equipment (or Third Party Hardware) to be operating satisfactorily as demonstrated by successful completion of diagnostic routines and is available for Customer's use; and (b) for Equipment (or Third Party Hardware) designated as "Customer Installable," the Equipment (or Third Party Hardware) delivery date.
- q. **Description of Services or DOS** means a document attached to an Order which references the applicable Services Contract number and specifies the Products and/or Services provided under such Order.
- r. **Diagnostic Software** means Xerox-proprietary software embedded in or loaded onto Equipment and used by Xerox to evaluate or maintain the Equipment.
- s. **Documentation** means all manuals, brochures, specifications, information and software descriptions, and related materials customarily provided by Xerox to customers for use with certain Products or Services.
- t. **Effective Date** means the date this Agreement is signed by Xerox.
- u. **Equipment** means Xerox-brand equipment.
- v. **Excluded Taxes** means (i) taxes on Xerox's income, capital, and employment, (ii) taxes for the privilege of doing business, and (iii) personal property tax on Equipment rented or leased to Customer under this Agreement.
- w. **Existing Equipment** means devices which are leased, rented or owned by the Customer outside of this Agreement, which are used to provide Services, and which remain subject to the terms and conditions of the agreements under which they were originally acquired.
- x. **Existing Software** means software licensed by the Customer outside of this Agreement and which is used to provide the Services and which remains subject to the terms and conditions of the agreements under which it was originally acquired.
- y. **Feature Releases** means new releases of Software that include new content or functionality.
- z. **Force Majeure Event** means a circumstance beyond a party's reasonable control, which circumstances include, but are not limited to, the following: act of God (e.g., flood, earthquake, wind); fire; war; act of a public enemy or terrorist; act of sabotage; strike or other labor dispute; riot; misadventure of the sea; inability to secure materials and/or transportation; or a restriction imposed by legislation, an order or a rule or regulation of a governmental entity.
- aa. **Funds** means collectively Amortized Services and Third Party Funds.
- bb. **Maintenance Releases or Updates** means new releases of Software that primarily incorporate coding compliance updates and error fixes and are designated as "Maintenance Releases" or "Updates."
- cc. **Maintenance Services** means required maintenance of Equipment to keep the Equipment in good working order.
- dd. **Module** means a specific set of terms and conditions contained in this Agreement that is identified as a "Module." The Modules under this Agreement are the DEF, GEN, SVC, EQP, EP, MS and SW Modules.
- ee. **Monthly Minimum Charge or MMC** means the regular recurring Charge that is identified in an Order and which, along with any additional print/impression charges, covers the cost for the Services, Maintenance Services, and/or Products. The MMC may also include lease buyout funds, Funds, monthly equipment component amounts, remaining Customer obligations from previous contracts, and amounts being financed or refinanced. One-time items are billed separately from the MMC.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

- ff. **Order** means a document that Xerox requires for processing of orders for Services, Maintenance Services and/or Products hereunder, which may specify the contracting parties and location(s) where the foregoing will be provided; Customer's requested shipment date; the Products that Customer will purchase, lease, rent or license; the Services and/or Maintenance Services that Xerox will provide; the applicable Charges and expenses; the term during which the Services, Maintenance Services and/or Products described therein shall be provided; the Xerox-provided contract number; and any applicable SLAs. An Order must reference the applicable Services Contract number, and may also be in the form of a Services and Solutions Order ("SSO"), a Xerox Order Agreement ("XOA") (which is used solely for an outright purchase by Customer under the EP module of this Agreement) or a Customer-issued PO. A Statement of Work may be part of an Order but cannot function as a stand-alone ordering document.
- gg. **Output of Services** means electronic images created by scanning tangible documents containing Customer Content, all full or partial copies (tangible and intangible) of Customer Content, and all reports and other documentation, photographs, images, impressions, and other materials (tangible and intangible) created by Xerox and delivered to Customer under an Order, but shall not include Third Party Software, or Xerox Intellectual Property.
- hh. **Privacy Laws** means laws relating to data privacy and data protection as applicable to Xerox's performance of the Services.
- ii. **Private Information** means Protected Health Information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), Non-Public Personal Information ("NPI") as defined by the Gramm-Leach Bliley Act ("GLBA") and equivalent categories of protected health and financial information under applicable state Privacy Laws.
- jj. **Products** means Software, Equipment, Third Party Products and/or Consumable Supplies supplied by Xerox and provided to Customer pursuant to an Order.
- kk. **Purchase Order or PO** means a document containing the applicable Services Contract number that is issued by Customer to Xerox for Order entry purposes only. Any terms in a PO are not binding and are of no force or effect.
- ll. **Purchased Equipment** means Equipment or Third Party Hardware that Xerox sells outright to Customer under the EP Module.
- mm. **Remote Data** means data that is automatically collected by Xerox or transmitted to or from Xerox by Equipment or Third Party Products connected to Customer's network. Examples of Remote Data include product registration, meter read, supply level, equipment configuration and settings, software version, and problem/fault code data.
- nn. **Remote Data Access** means electronic transmission of Remote Data to or from a secure offsite location.
- oo. **Residuals** means general ideas, concepts, know-how, methods, processes, technologies, algorithms or techniques related to the Services, which are in non-tangible form and retained in the unaided memory of persons who have had access to Confidential Information.
- pp. **Service Level Agreements or SLAs** means the levels of performance for the Services, if applicable, as set out in the applicable Order.
- qq. **Services** means managed services (e.g. copy center and mailroom services), consultative services, and/or professional services, including, but not limited to, assessment, document management, and managed and centralized print services, as more fully described in the applicable Order. Standard back-office administrative and contract support functions, such as billing, contract management and order processing, are not Services, but are included in the pricing provided for the Services hereunder.
- rr. **Services Contract** means the applicable terms and conditions of this Agreement, the first Order having a particular assigned Services Contract number, and each additional Order, if any, with the same Services Contract number.
- ss. **Software** means Base Software and Application Software.
- tt. **Statement of Work or SOW** means a document which references the applicable Services Contract number and specifies the details of a particular transaction where Customer wishes to acquire Services, Maintenance Services and/or Products from Xerox under this Agreement.
- uu. **Supplier Equipment** means devices which are supplied by Xerox to the Customer during the term of an Order. Supplier Equipment may be Equipment or Third Party Hardware.
- vv. **Taxes** means any and all taxes of any kind or nature, however denominated, imposed or collected by any governmental entity, including but not limited to federal, state, provincial, or local net income, gross income, sales, use, transfer, registration, business and occupation, value added, excise, severance, stamp, premium, windfall profit, customs, duties, real property, personal property, capital stock, social security, unemployment, disability, payroll, license, employee or other withholding, or other tax, of any kind whatsoever, including any interest, penalties or additions to tax or additional amounts in respect of the foregoing.
- ww. **Third Party Funds** means funds Xerox provides to Customer to acquire Third Party Hardware or to license Third Party Software and/or to retire debt on existing Third Party Hardware.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

- xx. **Third Party Hardware** means non-Xerox brand equipment.
- yy. **Third Party Products** means, collectively, Third Party Hardware and Third Party Software.
- zz. **Third Party Software** means non-Xerox brand software.
- aaa. **Transaction Taxes** means any and all Taxes that are required to be paid in respect of any transaction and resulting Charges under this Agreement and any transaction documents, including but not limited to sales, use, services, rental, excise, transaction-based gross receipts, and privilege Taxes.
- bbb. **XDM Customer Views** means a limited set of features such as printer error messages, basic printer status, troubleshoot (e.g., access printer web page, submit test page, reboot printer, retrieve audit logs) and upgrade printer (e.g., add upgrade file, delete upgrade file, run upgrade, delete upgrade task, restart upgrade task) that are available through the Xerox Tool known as Xerox Device Manager.
- ccc. **Xerox Confidential Information** means Confidential Information belonging to Xerox and includes, without limitation, whether marked as such or not, any services procedures manuals, Xerox Tools, Xerox Client Tools, and Xerox Intellectual Property.
- ddd. **Xerox Client Tools** means certain proprietary software used to provide certain Services, and any modifications, enhancements, improvements thereto and derivative works thereof that are licensed to Customer in accordance with GEN 1.8(d).
- eee. **Xerox Intellectual Property** means all intellectual property and associated intellectual property rights including patent, trademark, service mark, copyright, trade dress, logo and trade secret rights which exist and belong to Xerox as of the Effective Date or that may be created by Xerox after the Effective Date, including without limitation, Software, Data, Remote Data, Xerox Tools and Xerox Client Tools, and excluding Customer Confidential Information and Output of Services.
- fff. **Xerox Products** means Equipment, Software, and Consumable Supplies acquired pursuant to this Agreement.
- ggg. **Xerox Tools** means certain proprietary tools used by Xerox to provide certain Services, and any modifications, enhancements, improvements thereto and derivative works thereof.

GENERAL MODULE

GEN 1. – GENERAL

The terms and conditions in this General (GEN) Module apply to all Services, Maintenance Services, and Products acquired by Customer under this Agreement.

GEN 1.1– AGREEMENT STRUCTURE

- a. **General Contract Structure.** The parties intend for this Agreement to serve as a master agreement stating the terms and conditions governing separate transactions between (i) Xerox and Customer, and (ii) Xerox and Customer Affiliates. Xerox will provide, and Customer will procure, Services, Maintenance Services and/or Products in accordance with the terms and conditions stated in this Agreement, any Services Contract(s), and any applicable Orders.
- b. **Orders and Services Contracts.**
 - i. Xerox may accept Orders either by its signature or by commencing performance. Xerox reserves the right to review and approve Customer's credit, or in the case of an Order by a Customer Affiliate, such Affiliate's credit, prior to acceptance of an Order and the entity placing the Order hereby authorizes Xerox or its agent to obtain credit reports from commercial credit reporting agencies for this purpose. If a Customer Affiliate establishes a Services Contract by placing an Order hereunder, it will be the "Customer" for the purposes of such Services Contract.
 - ii. Orders for Services, Maintenance Services, and/or Products are grouped into Services Contracts. Each separate Services Contract will be established when the first Order is placed that bears a new Services Contract number assigned by Xerox and Xerox accepts that Order. Each Services Contract will be assigned its own Services Contract number that will consist of this Agreement's number followed by a three digit extension. Each Services Contract constitutes a separate contract under this Agreement. Customer may add Services, Maintenance Services, or Products to an existing Services Contract by submitting additional Orders referencing the applicable Services Contract number. Each Services Contract will consist of the terms and conditions of this Agreement, the first Order under the Services Contract number and each additional Order with the same Services Contract number.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

- iii. Unless Customer provides notice in writing at least thirty (30) days before the end of the term of an Order of its intention not to renew, the Order will renew automatically on a month-to-month basis on the same terms and at the same price.
- iv. Orders may be submitted by hard copy or electronic means and those submitted electronically will be considered: (a) a "writing" or "in writing;" (b) "signed" by the Customer; (c) an "original" when printed from electronic records established and maintained in the ordinary course of business; and (d) valid and enforceable.

GEN 1.2 – CHARGES, PAYMENT AND DEFAULT

- a. **Charges.** Charges for the particular Services, Maintenance Services, and/or Products will be set forth in an Order and are exclusive of any and all Transaction Taxes. Xerox's then current overtime rates will apply to Services requested and performed outside Customer's standard working hours.
- b. **Payment.** Customer agrees to pay Xerox all undisputed amounts due under each invoice via check, Automated Clearing House debit, Electronic Funds Transfer, or direct debit from Customer's bank account within thirty (30) days after the invoice date. Restrictive covenants submitted for or with payment to indicate that it is in full satisfaction of an invoice will not operate as an accord and satisfaction to reduce Customer's payment obligations if it is not, in fact, full payment. For any payment not received by Xerox within ten (10) days after the due date, Xerox may charge, and Customer agrees to pay, a late charge of the greater of \$25 or five percent (5.0%) of the amount overdue (not to exceed the maximum amount permitted by applicable law) as reasonable collection costs. If Customer disputes any amount included in an invoice, then (i) Customer must notify Xerox of the dispute in writing, (ii) such notice shall include a description of the items Customer is disputing and the reason such items are being disputed; and (iii) Customer shall promptly exercise its best efforts to work with Xerox to resolve such dispute. Pending resolution of such disputed amount, Customer shall pay any and all undisputed amounts within thirty (30) days of invoice date, including the MMC which Customer agrees shall not be subject to dispute at any time.
- c. **Default.** Customer will be in default if Xerox does not receive any payment within fifteen (15) days after the date it is due, or if Customer breaches any other obligation under this Agreement, any Services Contract, or any other agreement with Xerox. If Customer, defaults, Xerox, in addition to its other remedies (including cessation of Services, Maintenance Services and/ or Consumable Supplies), may require immediate payment of (1) all amounts then due, plus interest on all amounts due from the due date until paid at the rate of 1.5% per month, and (2) any early termination charges set forth in this Agreement or in the applicable Services Contract and/or Order(s). Customer will pay all reasonable costs, including attorneys' fees, incurred by Xerox to enforce any Services Contract.

GEN 1.3 – TAXES

- a. Customer will be responsible for all Transaction Taxes. Transaction Taxes will be included in Xerox's invoice unless Xerox receives proof of Customer's tax-exempt status. Customer shall not be responsible for Excluded Taxes.

GEN 1.4 – RESERVED.

GEN 1.5 – RESERVED.

GEN 1.6 – CUSTOMER RESPONSIBILITIES

Customer agrees to perform its responsibilities under this Agreement in support of the Services, Maintenance Services, or Products in a timely manner. Customer agrees:

- a. that Products acquired hereunder are ordered for Customer's (or its Affiliates') own internal business use (rather than resale, license and/or distribution outside of Customer's organization) and will not be used for personal, household or family purposes;
- b. to (1) provide Xerox and its agents with timely and sufficient access, without charge, to Customer Facilities required by Xerox to perform Services and Maintenance Services and/or provide Products, and (2) ensure that Customer Facilities are suitable for the Services, Maintenance Services and/or Products, safe for Xerox personnel, and fully comply with all applicable laws and regulations, including without limitation any federal, state and local building, fire and safety codes;
- c. to provide Xerox and its agents with timely and sufficient use of and access, without charge, to Customer Assets required by Xerox to perform Services and Maintenance Services and/or provide Products, and to grant Xerox and its agents sufficient rights to use, access and, if agreed, modify the same;
- d. to acquire or continue maintenance, repair and software support services, without charge to Xerox, for all Customer Assets that Customer permits Xerox to use or access;
- e. to maintain the manufacturer's maintenance agreement for any Third Party Products;

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

- f. to provide Xerox with access to appropriate members of Customer personnel, as reasonably requested by Xerox, in order for Xerox to perform the Services and Maintenance Services and/or provide Products;
- g. to respond to and provide such documentation, data and other information as Xerox reasonably requests in order for Xerox to perform the Services and Maintenance Services and/or provide Products;
- h. to contract for the minimum types and quantities of Equipment and Consumable Supplies required by Xerox to perform the Services and Maintenance Services;
- i. that, as between Xerox and Customer, Customer alone is responsible for backing up its Customer Content and Xerox shall not be responsible for Customer's failure to do so;
- j. that as between Xerox and Customer, Customer alone is responsible for determining whether Customer Content provided to Xerox (i) is libelous, defamatory or obscene, or (ii) may be duplicated, scanned or imaged without violating a third party's intellectual property rights; and
- k. to provide contact information for Equipment such as name and address of Customer contact.

GEN 1.7- WARRANTIES

- a. **Mutual Warranties.** Each party represents and warrants to the other, as an essential part of this Agreement, that:
 - i. it is duly organized and validly existing and in good standing under the laws of the state or country of its incorporation or formation;
 - ii. this Agreement and the Orders hereunder have been duly authorized by all appropriate corporate action for signature; and
 - iii. the individual signing this Agreement, and all Orders (where applicable), is duly authorized to do so.
- b. **Xerox Warranties.**
 - i. Services Warranty. Xerox warrants to the Customer that the Services will be performed in a professional and workmanlike manner by Xerox personnel with appropriate training, experience and skills in accordance with the applicable Order. If the Services do not comply with the SLAs or other requirements set forth in the applicable Order, Customer will notify Xerox in writing detailing its concerns and, within 10 days following Xerox's receipt of such notice, Xerox and Customer will meet, clarify the Customer's concern(s), and begin to develop a corrective action plan. As Customer's exclusive remedy under this warranty for Xerox's non-compliance with this warranty, Xerox will either modify the Services to comply with the applicable SLAs or other requirements or re-do the work at no additional charge within 60 days of finalizing the plan or another time period agreed to in writing by the parties.
 - ii. Equipment Warranty. Any Equipment warranty to which Customer is entitled shall commence upon the Date of Installation. Use by Customer of consumables not approved by Xerox that affect the performance of the Equipment may invalidate any applicable warranty.
 - iii. Third Party Product Warranty. Where Xerox in its sole discretion selects and supplies Third Party Products, Xerox warrants they will operate substantially in conformance with applicable SLAs or other requirements in the Order. Customer's sole remedy for breach of this warranty is to return the Third Party Product to Xerox and then receive a refund of any fees paid for such non-conforming Third Party Product, less a reasonable usage fee. If Customer requests a specific Third Party Product, Xerox will pass-through as permitted any third party warranties.
 - iv. Exclusions. Xerox shall not be responsible for any delay or failure to perform the Services or provide Products, including achieving any associated SLAs or other requirements in the applicable SOWs, DOSs or Orders, to the extent that such delay or failure is caused by:
 - (a) Customer's failure or delay in performing its responsibilities under this Agreement;
 - (b) reasons outside Xerox's reasonable control, including Customer Assets, Customer Content, or delays or failures by Customer's agents, suppliers or providers of maintenance and repair services for Customer Assets; or
 - (c) unauthorized modifications to Equipment, Third Party Hardware or the Output of Services.
- c. **Disclaimer.** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, AND XEROX DISCLAIMS AND CUSTOMER WAIVES ALL OTHER WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. EXCEPT AS EXPRESSLY PROVIDED HEREIN AND AS PERMITTED BY APPLICABLE LAW, CUSTOMER WAIVES ALL

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

RIGHTS AND REMEDIES CONFERRED UPON A LESSEE BY ARTICLE 2A OF THE UNIFORM COMMERCIAL CODE.

- d. The warranties set forth in this Agreement are expressly conditioned upon the use of the Services, Products and Output of Services for their intended purposes in the systems environment for which they were designed and shall not apply to any Services, Products or Output of Services which have been subject to misuse, accident or alteration or modification by Customer or any third party.

GEN 1.8 – INTELLECTUAL PROPERTY OWNERSHIP

- a. **Customer Intellectual Property.** Customer grants to Xerox a non-exclusive, royalty-free, fully-paid up, worldwide license to use Customer Intellectual Property, Customer Content and Output of Services only for purposes of, and only to the extent required for, providing Services, Maintenance Services or Products under this Agreement. Xerox agrees not to decompile or reverse engineer any Customer Intellectual Property. Except as expressly set forth in this Agreement, no rights to any Customer Intellectual Property are granted to Xerox.
- b. **Ownership of Output of Services and License to Xerox Intellectual Property.** Except to the extent that the Output of Services may incorporate any Xerox Intellectual Property, the Output of Services shall be the sole and exclusive property of Customer. To the foregoing extent, Xerox hereby assigns, grants, conveys, and transfers to Customer all rights in and to the Output of Services for the applicable Order. To the extent that the Output of Services may incorporate any Xerox Intellectual Property, Xerox grants Customer a non-exclusive, perpetual, fully paid-up, worldwide right to use, display, and reproduce the Xerox Intellectual Property only as required for use of the Output of Services for Customer's customary business purposes and not for resale, license or distribution outside of Customer's organization. If XDM Customer Views are to be provided under a SOW, Xerox grants Customer a limited license to access and use the XDM Customer Views only for the purpose of receiving Services under the SOW. Customer agrees not to decompile or reverse engineer any Xerox Intellectual Property. Except as expressly set forth in this Agreement, no rights to any Xerox Intellectual Property are granted to Customer.
- c. **Xerox Tools.** Xerox Tools may be used by Xerox to provide certain Services. Xerox and its licensors will at all times retain all right, title and interest in and to Xerox Tools including without limitation, all intellectual property rights therein, and, except as expressly set forth herein, no rights to use, access or operate the Xerox Tools are granted to Customer. Xerox Tools will be installed and operated only by Xerox or its authorized agents. Customer will not decompile or reverse engineer any Xerox Tools, or allow others to engage in same. Customer will have access to Data and reports generated by the Xerox Tools and stored in a provided database as set forth in the applicable SOW. Xerox may remove Xerox Tools at any time in Xerox's sole discretion, provided that the removal of Xerox Tools will not affect Xerox's obligations to perform Services, and Customer shall reasonably facilitate such removal.
- d. **Xerox Client Tools.** Xerox grants to Customer a non-exclusive, non-transferable, non-assignable (by operation of law or otherwise) license to install, use and access the Xerox Client Tools only for the purpose of receiving the Services for which they were provided. Customer may not: (i) distribute, copy, modify, create derivatives of, decompile, or reverse engineer the Xerox Client Tools, except as permitted by applicable law; or, (ii) allow others to engage in same. Title to the Xerox Client Tools and all intellectual property rights therein shall, at all times, reside solely with Xerox and its licensors. Certain Xerox Client Tools may be subject to mandatory third party flow-down terms and conditions, which will be provided separately.
- e. **Data Collection and Use.** Data collected by the Xerox Tools is transmitted by a Xerox Tool to a remotely hosted server that hosts other Xerox Tools. The automatic data transmission capability will not allow Xerox to read, view or download any Customer documents or other information residing on or passing through the Equipment or Third Party Hardware or Customer's information management systems.

GEN 1.9 – INDEMNIFICATION

- a. **General Indemnification.** Xerox, if promptly notified and given the right to control the defense, shall indemnify, defend and hold harmless the Customer, its Affiliates, and their respective officers, directors, employees, agents, successors and assigns, from and against all claims by a third party for losses, damages, costs or liability of any kind (including expenses and reasonable legal fees) that a court finally awards such party ("Claims") for bodily injury (including death) and damage to real or tangible property, to the extent proximately caused by Xerox's negligent acts or omissions, or willful misconduct in connection with this Agreement.
- b. **Xerox Indemnification.** Xerox shall, if promptly notified by Customer (or its Affiliate(s)) and given the right to control the defense, indemnify, defend and hold harmless Customer, its Affiliates and their respective officers, directors, employees, agents successors and assigns, for all Claims that Xerox Products or Customer's use of the Services provided by Xerox under this Agreement infringe a U.S. patent, copyright or other intellectual property right. Notwithstanding anything to the contrary herein, Xerox shall have no obligation under this Section **GEN 1.9(b)** to the extent any Claim is based on or arises out of any (i) Services performed using Customer Assets, Customer Content

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

or other materials provided to Xerox by Customer for which Customer failed to provide sufficient rights to Xerox; (ii) infringement by Services resulting from Customer's direction, specification or design, (iii) modification or alteration to such Xerox Products or Services not approved in writing by Xerox; (iv) any combination or use of the Xerox Products or Services not approved in writing by Xerox; (v) use of the Xerox Products or Services not in accordance with the applicable Documentation; or (vi) Customer's failure to use corrections or enhancements to the Xerox Products provided by Xerox. If a Claim is made or appears likely to be made pursuant to this Section **GEN 1.9(b)**, Customer agrees to permit Xerox, at Xerox's sole option and expense, to obtain the right to enable Customer to continue to use such Xerox Products, to make them non-infringing or to replace them with items that are at least functionally equivalent. If Xerox determines that none of these alternatives is reasonably available, Customer agrees to return such Xerox Products to Xerox upon Xerox's written request. Xerox will then give Customer a refund equal to the amount Customer paid Xerox for such Xerox Products less a reasonable usage fee.

- c. Xerox is not responsible for any litigation expenses of the Customer or any settlements unless it pre-approves them in writing.

GEN 1.10 – LIMITATION OF LIABILITY

Except as prohibited by law, the following limitations apply:

- a. **NO CONSEQUENTIAL DAMAGES.** SUBJECT TO SECTION **GEN 1.10(c)**, IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES OR THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES OR AGENTS BE LIABLE TO THE OTHER PARTY OR ITS AFFILIATES OR THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES OR AGENTS FOR ANY INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, AND EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
- b. **LIMITATION ON RECOVERY.** SUBJECT TO SECTION **GEN 1.10(c)**, THE TOTAL AGGREGATE LIABILITY OF EITHER PARTY (AND ITS AFFILIATES AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES OR AGENTS) FOR DIRECT DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, WILL BE LIMITED TO AN AMOUNT EQUAL TO THE AMOUNT OF ALL CHARGES PAID BY CUSTOMER TO XEROX UNDER THE ORDER UNDER WHICH THE CLAIM AROSE (LESS PASS THROUGH EXPENSES SUCH AS, WITHOUT LIMITATION, POSTAGE) IN THE TWELVE (12) MONTHS PRIOR TO THE DATE UPON WHICH THE CLAIM AROSE. THE EXISTENCE OF MULTIPLE CLAIMS OR SUITS UNDER OR RELATED TO THIS AGREEMENT AND ANY ORDERS HEREUNDER WILL NOT ENLARGE OR EXTEND THIS LIMITATION OF DAMAGES. NOTWITHSTANDING THE FOREGOING, NOTHING SET FORTH IN THIS SECTION **GEN 1.10(b)** SHALL LIMIT CUSTOMER'S OBLIGATION TO PAY XEROX ALL CHARGES AND EXPENSES FOR PRODUCTS AND SERVICES PROVIDED UNDER THIS AGREEMENT.
- c. **EXCEPTIONS.** THE LIMITATIONS SET FORTH IN SECTION **GEN 1.10** SHALL NOT APPLY WITH RESPECT TO:
- i. THE SPECIFIC INDEMNITY OBLIGATIONS SET OUT IN THIS AGREEMENT;
 - ii. EITHER PARTY'S WILLFUL MISCONDUCT, GROSS NEGLIGENCE OR FRAUD;
 - iii. BODILY INJURY OR DEATH CAUSED BY A PARTY'S NEGLIGENCE OR WILLFUL MISCONDUCT OR THAT OF ITS EMPLOYEES, AGENTS OR SUBCONTRACTORS; OR
 - iv. A PARTY EXCEEDING ITS RIGHTS, IF ANY, TO THE OTHER PARTY'S INTELLECTUAL PROPERTY OR MISAPPROPRIATING OR INFRINGING THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS AS GRANTED UNDER THIS AGREEMENT.

GEN 1.11 – TERM AND TERMINATION

This Agreement shall commence on the Effective Date and shall continue for a term of _____ months, and continue on a month-to-month basis thereafter until expressly renewed by mutual written agreement or terminated by either party upon thirty (30) days' written notice. Upon termination, Customer shall permit Xerox to enter Customer Facilities for purposes of removing the Products, Xerox Tools, and/or Xerox Client Tools. Each Order hereunder shall have its own term, which shall be stated in the Order. In the event that the Region 4 ESC Contract expires or is terminated, this Agreement and all Services Contracts and Orders thereunder that are in effect at that time shall remain in full force and effect until their expiration or termination, and continue under the same terms and conditions as if the Region 4 ESC Contract were still in effect. In the event this Agreement expires or is terminated, each Services Contract in effect at that time shall remain in full force and effect until the expiration or termination of all Orders constituting such Services Contract (including any extensions or renewals thereof) and shall at all times be governed by, and be subject to, the terms and conditions of this Agreement as if this Agreement were still in effect. Termination of any Order shall not affect this Agreement or any other Orders then in effect. Notwithstanding any other provision in the

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

Agreement to the contrary, should an Order be terminated prior to expiration for any reason or a unit of Third Party Hardware or any Third Party Software for which Third Party Funds have been provided is removed or replaced prior to expiration, Customer agrees to pay to Xerox, in addition to any other amounts owed under said Order, an amount equal to the remaining principal balance of the Funds together with a 15% disengagement fee, for loss of bargain and not as a penalty.

GEN 1.12– CONFIDENTIALITY

- a. **Obligation.** Customer and Xerox acknowledge that, during the term of this Agreement and any Order hereunder, each party (or its Affiliates) may be provided with or have access to, certain Confidential Information belonging to the other party (or its Affiliates). The parties will ensure that their employees comply with their respective corporate policies and procedures regarding the disclosure of Confidential Information. The parties agree to use the Confidential Information provided under this Agreement only for purposes directly related to the performance of obligations and use of rights granted under this Agreement. The receiving party may not disclose Confidential Information to third parties unless such third party has a need to know such Confidential Information in order to perform under this Agreement and has agreed in writing to be bound by terms no less restrictive than those set forth herein. Each party shall be responsible for any breaches of the obligations in this Section by its employees and such third parties. The receiving party shall protect the disclosing party's Confidential Information with the same degree of care that it uses to protect its own confidential information of like importance, but not less than reasonable care. Each party agrees not to disclose the terms and conditions of this Agreement, all Services Contracts and Orders, and any attachments and exhibits thereto, without the other party's prior written consent. Xerox may use Customer as a reference with other customers, including in marketing materials. Xerox may disclose the identity and address of Customer to Xerox's third party licensors if contractually required for royalty reporting purposes.
- b. **Exclusions.** The obligations of confidentiality will not apply to any Confidential Information that: (1) was in the public domain prior to, at the time of, or subsequent to the date of disclosure through no fault of the receiving party; (2) was rightfully in the receiving party's possession or the possession of any third party free of any obligation of confidentiality; or (3) was developed by the receiving party's employees independently of and without reference to any of the other party's Confidential Information.
- c. **Return of Information.** Upon termination or expiration of this Agreement or an Order, except as otherwise set forth hereunder, each party shall cease use of the other party's Confidential Information and other data and, upon request, shall (1) return all such Confidential Information and any copies thereof, or (2) permanently destroy such Confidential Information and certify that such Confidential Information has been so destroyed; provided, however, that any obligations regarding removal of Customer Confidential Information stored on hard drives on Equipment owned by Xerox and any costs associated with such removal will be set forth in the applicable Order.
- d. **Disclosure under Legal Requirement.** If the recipient of Confidential Information is required to disclose Confidential Information pursuant to a court order or by law or regulation, that party will (1) notify the disclosing party of the obligation to make such disclosure, and (2) reasonably cooperate with the disclosing party if the disclosing party seeks a protective order, but any costs incurred by the receiving party will be reimbursed by the disclosing party, except for costs of the receiving party's employees.
- e. **Duration of Confidentiality Obligation.** Except for Private Information and Xerox Intellectual Property, the obligations set forth in this Section shall continue for one (1) year after termination or expiration of this Agreement or the Order under which such Confidential Information was disclosed, whichever occurs later. The duration of confidentiality obligations with respect to Private Information shall be governed by applicable Privacy Laws. Confidentiality obligations with respect to Xerox Intellectual Property shall continue so long as it continues to be Xerox trade secrets.
- f. **Residual Rights.** Each party understands that the other party shall be free to use for any purpose the Residuals resulting from access to Confidential Information as a result of the performance of its obligations under an Order, provided that such party shall maintain the confidentiality of such Confidential Information as provided herein. Neither party shall pay royalties for the use of Residuals. However, the foregoing shall not be deemed to grant either party a license under the other party's copyrights or patents.

GEN 1.13– DATA PROTECTION/PRIVACY

- a. To the extent that Privacy Laws are applicable to Customer and Xerox in connection with the performance of Services, each party agrees to comply with the applicable provisions of such Privacy Laws.
- b. Xerox has adopted reasonable physical, technical, and organizational safeguards designed to prevent accidental, unauthorized, or unlawful loss, disclosure, access, transfer or use of Private Information. Xerox will promptly notify Customer in the event of any known unauthorized or unlawful loss, disclosure, access, transfer, or use of Private Information.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

GEN 1.14 – GOVERNING LAW AND JURISDICTION

This Agreement, each respective Order, and any dispute or claim arising out of or in connection with this Agreement or such Order, shall be governed by and construed in accordance with the laws of New York without regard to its conflict of laws provisions and submitted to the exclusive jurisdiction of the federal and state courts of New York.

GEN 1.15 – RESERVED.

GEN 1.16– FORCE MAJEURE

Except for Customer's absolute and unconditional obligation to make all required payments of any amounts not properly disputed under this Agreement, neither Customer nor Xerox shall be liable to the other party during any period in which its performance is delayed or prevented, in whole or in part, by a Force Majeure Event. If such a circumstance occurs, the party whose performance is delayed or prevented shall undertake reasonable action to notify the other party thereof.

GEN 1.17 – INSURANCE COVERAGE

Xerox shall maintain the following limits of insurance coverage during the term of this Agreement:

1. Where required by law, Workers Compensation, at statutory limits;
2. Employers Liability, with \$1,000,000 USD limit of liability or at statutory limits, whichever is greater;
3. Commercial General Liability, including Products - Completed Operations coverage and Broad Form Contractual, with \$2,000,000 USD limit of liability per occurrence for Bodily Injury and Property Damage; and,
4. Where applicable, Automobile Liability, with a combined single limit of liability of \$2,000,000 USD per accident or at statutory limits, whichever is greater.

GEN 1.18 – FUNDING (this provision applies to state & local government Customers only)

Customer represents and warrants that all payments due and to become due during Customer's current fiscal year are within the fiscal budget of such year and are included within an unrestricted and unencumbered appropriation currently available for the acquisition of the Products, and it is Customer's intent to use the Products for the entire initial term and to make all payments required under the Agreement or an Order. If (i) through no action initiated by Customer, Customer's governing body does not appropriate funds for the continuation of the Agreement or an Order for any fiscal year after the first fiscal year and has no funds to do so from other sources, and (ii) Customer has made a reasonable but unsuccessful effort to find an assignee within Customer's general organization who can continue the Agreement or an Order, the Agreement or the Order may be terminated. To effect this termination, Customer must, 30 days prior to the beginning of the fiscal year for which Customer's governing body does not appropriate funds for the upcoming fiscal year, notify Xerox that Customer's governing body failed to appropriate funds and that Customer has made the required effort to find an assignee. Customer's notice must certify that canceled Equipment is not being replaced by equipment performing similar functions during the ensuing fiscal year. Customer agrees to release the Equipment to Xerox and, when returned, the Equipment will be in good condition and free of all liens and encumbrances. Customer will then be released from any further payments obligations beyond those payments due for the current fiscal year.

GEN 1.19– COMPLIANCE WITH LAWS AND POLICIES

Xerox and Customer shall comply with all applicable laws and regulations in the performance of their respective obligations under this Agreement. Xerox agrees to comply with Customer's internal policies regarding security and safety at Customer Facilities that are reasonable and customary under the circumstances and which do not conflict with the terms of this Agreement. Customer agrees to provide Xerox with reasonable prior written notice of such policies and any changes to such policies. If a change in Customer policy results in incremental costs to Xerox, Xerox may, upon providing notice to Customer, pass such costs on to Customer.

GEN 1.20 – MISCELLANEOUS

- a. **Copies of Agreement.** Except as required by law, both parties agree that any reproduction of this Agreement made by reliable means (for example, photocopy or facsimile) shall be considered an original. Xerox may retain a hardcopy, electronic image, photocopy, or facsimile of this Agreement and each Order hereunder, which shall be considered an original and shall be admissible in any action to enforce said Agreement or Order.
- b. **Amendment.** All changes to this Agreement must be made in a writing signed by Customer and Xerox. Any amendment of this Agreement shall not affect the obligations of either party under any then-existing Orders, which shall continue in effect unless the amendment expressly states that it applies to such existing Orders. An amendment to a Services Contract shall reference the number of the Services Contract that it amends.
- c. **No Waiver; Severability; Survival.** The failure by Customer or Xerox to insist upon strict performance of any of the terms and conditions in this Agreement or to exercise any rights or remedies will not be construed as a waiver of the right to assert those rights or to rely on that term or condition at any time thereafter. If any provision is held invalid by any arbitrator or any court under applicable law, such provision shall be deemed to be restated as nearly as

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

possible to reflect the original intention of the parties in accordance with applicable law. The remainder of this Agreement shall remain in full force and effect. Any terms and conditions of this Agreement or any Order which by their nature extend beyond the termination or expiration of the Agreement or Order will survive such termination or expiration.

- d. **Independent Contractors.** Xerox shall perform all Services hereunder in the capacity of independent contractor and not as Customer's employee, agent, or representative. Xerox employees shall not be entitled to privileges of employment that Customer may provide to Customer's employees, and Xerox shall be responsible for payment of all unemployment, social security, federal (state and local, as necessary) and other payroll taxes in regard to its employees involved in the performance of the Services. Neither of the parties, nor their respective employees or Affiliates, shall be authorized to conclude contracts in the name of the other party, or to act or appear as a representative of the other, whether in performing the Services or otherwise.
- e. **No Hiring.** During the term of an Order under which Xerox is providing Services and for a period of one (1) year thereafter, Customer and Xerox each agree not to hire, solicit, or employ any of the other's personnel who have been engaged in the provision of services or the performance of this Agreement, unless prior written consent is obtained from the other party. Such prohibition shall not apply to hiring as a result of general public solicitations of employment. Should one of the parties hire the other party's personnel in violation of this Agreement, the violating party shall immediately pay to the other, as liquidated damages and as the sole remedy for such violation, an amount equal to such personnel's then current annual compensation (or the amount paid to such person during the previous twelve (12) months in the case of an independent contractor).
- f. **Assignment.** Except for Xerox's assignment to an Affiliate or to a third party for the purposes of securitizing or factoring, neither party may assign this Agreement and any Order(s) hereunder without the prior written consent of the other party. In the event of a permitted assignment by Xerox, each successive assignee of Xerox will have all of the rights but none of the obligations of Xerox pursuant to this Agreement. Customer will continue to look to Xerox for performance of Xerox's obligations hereunder and Customer hereby waives and releases any assignees of Xerox from any such claim. Customer will not assert any defense, counterclaim, or setoff that Customer may have or claim against Xerox against any assignee of Xerox.
- g. **Communication Authorization.** Customer authorizes Xerox or its agents to communicate with Customer by any electronic means (including cellular phone, email, automatic dialing, and recorded messages) using any phone number (including cellular) or electronic address that Customer provides to Xerox.
- h. **Limitation on Charges.** In no event will Xerox charge or collect any amounts in excess of those allowed by applicable law. Any part of an Order that would, but for this Section, be construed to allow for a charge higher than that allowed under any applicable law, is limited and modified by this Section to limit the amounts chargeable under such Order to the maximum amount allowed by law. If, in any circumstances, an amount in excess of that allowed by law is charged or received, such charge will be deemed limited to the amount legally allowed and the amount received by Xerox in excess of that legally allowed will be applied to the payment of amounts owed or will be refunded to Customer.
- i. **Order of Precedence; Entire Agreement.** This Agreement, including all schedules, attachments, exhibits and amendments hereto and the Services Contract(s) hereunder, and the Region 4 ESC Contract, constitutes the entire agreement between the parties as to the subject matter and supersedes all prior and contemporaneous oral and written agreements regarding the subject matter hereof and neither party has relied on or is relying on any other information, representation, discussion or understanding in entering into and completing the transactions contemplated in this Agreement. The parties agree that except as expressly set forth in this Agreement, in the event of any conflict between terms and conditions, the order of precedence shall be this Agreement, the applicable Orders under the Services Contract (excluding Customer POs), the SOW or DOS, as applicable, and the Region 4 ESC Contract. If a term in this Agreement expressly provides for a term in an Order to take precedence, such provision in the Order shall prevail to the extent of any conflict. Notwithstanding the foregoing, provisions in the General Module of this Agreement related to: (1) Section **GEN 1.8** (Intellectual Property Ownership); (2) Section **GEN 1.9** (Indemnification); (3) Section **GEN 1.10** (Limitation of Liability); (4) Section **GEN 1.12** (Confidentiality); and (5) Section **GEN 1.3** (Taxes), will prevail over conflicting provisions in any other contractual document.

SERVICES MODULE

SVC 1 – TERMS AND CONDITIONS SPECIFIC TO SERVICES

In addition to the terms and conditions in the General (GEN) Module, the following terms and conditions apply to Xerox's performance of Services.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

SVC 1.1 – SCOPE OF SERVICES

Subject to the terms and conditions of this Agreement, Services will be performed by Xerox and/or its Affiliates in accordance with the requirements set forth in an Order. If Customer fails to perform or is delayed in performing any of its responsibilities under this Agreement, such failure or delay may prevent Xerox from being able to perform any part of the Services or Xerox-related activities. Xerox shall be entitled to an extension or revision of the applicable term of the Order (which may include setting a new expected date for commencement of Services) or to an equitable adjustment in performance metrics associated with such failure or delay.

SVC 1.2 – CHARGES FOR SERVICES

Charges for Services are set forth in the applicable Order. Charges are based upon information exchanged between Customer and Xerox, which is assumed to be complete and accurate, and also depend upon other factors such as the timely performance by Customer of its responsibilities. If: (a) such information should prove to be incomplete or inaccurate in any material respect; or (b) there is a failure or delay by the Customer in performing its responsibilities under this Agreement or an Order which results in Xerox incurring a loss or additional cost or expense, then the charges shall be adjusted to reflect proportionately the impact of such materially incomplete or inaccurate information or such failure or delay. Charges that are indicated in an Order as being fixed are not subject to an annual percentage escalation for the initial term of such Order. If Xerox provides Services partially or early (for example, prior to the start of the initial term of an Order), Xerox will bill Customer on a pro rata basis, based on a thirty (30) day month, and the terms and conditions of this Agreement will apply.

SVC 1.3 – USE OF SUBCONTRACTORS

Xerox may, when it reasonably deems it appropriate to do so, subcontract any portion of the Services. Xerox shall remain responsible for any Services performed by subcontractors retained by Xerox to the same extent as if such Services were performed by Xerox.

SVC 1.4 – SERVICES SCOPE CHANGES

Except as otherwise set forth in an Order, either party may propose to modify the then-existing Services that are described in an Order, or to add new Services under a Services Contract. If Xerox determines such changes are feasible, Xerox will prepare and propose to Customer an Order incorporating the requested changes and any related impact to the Charges or terms. Once Customer executes and Xerox accepts the Order, Xerox will promptly proceed with the new and/or revised Services in accordance with the terms of the Order and this Agreement.

SVC 1.5 – EARLY TERMINATION OF SERVICES AND LABOR

Except as otherwise set forth in a Services Contract, upon ninety (90) days prior written notice, Customer may terminate or reduce any Services or labor provided pursuant to an Order without incurring early termination charges except as set forth in the next sentence. Notwithstanding the foregoing, if any such Services or labor provided under an Order are terminated (a) by Xerox due to Customer's default or (b) by Customer and Customer acquires similar services from another supplier within six (6) months of the termination of such Services or labor, Customer shall pay all amounts due as of the termination date, together with the early termination charges, for loss of bargain and not as a penalty, stated in the Order or, if not specifically stated therein, an amount equal to the then current MMC for said terminated or reduced Services or labor multiplied by the number of months remaining in the term of the related Order, not to exceed six (6) months.

EQUIPMENT MODULE

EQP 1 – TERMS AND CONDITIONS SPECIFIC TO EQUIPMENT & THIRD PARTY HARDWARE

In addition to the terms and conditions in the General (GEN) Module, the following terms and conditions apply to Equipment and Third Party Hardware provided to Customer.

EQP 1.1 – TERM AND DATE OF INSTALLATION

The term for each unit of Equipment shall be the term stated on the applicable Order, with the commencement date based upon the actual Date of Installation. If the Date of Installation for a unit of Equipment is prior to the applicable Order start date, Xerox will bill the Customer for such Equipment on a pro rata basis, based on a thirty (30) day month, and the terms and conditions of this Agreement and the applicable Services Contract will apply as of the Date of Installation.

EQP 1.2 – DELIVERY AND REMOVAL AND SUITABILITY OF CUSTOMER FACILITIES

Xerox will be responsible for all standard delivery charges for Equipment and Third Party Hardware and, for Equipment or Third Party Hardware for which Xerox holds title, standard removal charges. Non-standard delivery or removal charges (including removal prior to the end of the term for any Equipment) will be at Customer's expense. The suitability of Customer Facilities for installation of Equipment or Third Party Hardware, including compliance with state and local building, fire and safety codes and any non-standard state or local installation requirements, is Customer's responsibility.

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

EQP 1.3 – EQUIPMENT STATUS

Unless Customer is acquiring previously installed equipment, Equipment will be either: (a) “Newly Manufactured,” which may contain some recycled components that are reconditioned; (b) “Factory Produced New Model” which is manufactured and newly serialized at a Xerox factory, adds functions and features to a product previously disassembled to a Xerox predetermined standard, and contains new components and recycled components that are reconditioned; or (c) “Remanufactured,” which has been factory produced following disassembly to a Xerox predetermined standard and contains both new components and recycled components that are reconditioned. Xerox makes no representations as to the status of any Third Party Hardware that Xerox may provide under any Order.

EQP 1.4 – CONSUMABLE SUPPLIES

If specified in an Order, Xerox will provide Consumable Supplies for related Equipment. Consumable Supplies are Xerox's property until used in the Equipment for which they are provided. Upon expiration or termination of the applicable Order, Customer will either return any unused Consumable Supplies to Xerox at Xerox's expense when using Xerox-supplied shipping labels, or destroy them in a manner permitted by applicable law. Xerox reserves the right to charge Customer for any Consumable Supplies usage that exceeds Xerox's published yields by more than ten percent (10%). In such a case, Xerox will notify Customer of the excess usage. If such excess usage does not cease within thirty (30) days after notice, Xerox may charge Customer for the excess usage. If Xerox provides paper under a Services Contract, upon thirty (30) days' notice, Xerox may adjust paper pricing or either party may terminate the provision of paper.

EQP 1.5 – USE AND RELOCATION

For any Equipment or Third Party Hardware provided by Xerox, with the exception of Purchased Equipment for which Customer has paid in full, Customer agrees that: (a) the Equipment or Third Party Hardware shall remain personal property; (b) Customer will not attach any of the Equipment or Third Party Hardware as a fixture to any real estate; (c) Customer will not pledge, sub-lease or part with possession of the Equipment or Third Party Hardware or file or permit to be filed any lien against the Equipment or Third Party Hardware; and (d) Customer will not make any permanent alterations to the Equipment or Third Party Hardware. While Equipment or Third Party Hardware is subject to an Order, Customer must provide Xerox prior written notice of all Equipment or Third Party Hardware relocations and Xerox may arrange to relocate the Equipment or Third Party Hardware at Customer's expense. While Equipment or Third Party Hardware is being relocated, Customer remains responsible for making all payments to Xerox required under the applicable Order. All parts or materials replaced, including as part of an upgrade, will become Xerox's property. Equipment or Third Party Hardware cannot be relocated outside of the U.S. until Customer has paid in full for the Equipment or Third Party Hardware and has received title thereto. Notwithstanding anything to the contrary in the foregoing, to the extent the Equipment contains any Software, any relocation of such Equipment is subject to the terms and conditions set forth in the Software License Module of this Agreement.

EQP 1.6 – SUPPLIER EQUIPMENT PROVIDED

In the event Xerox provides Supplier Equipment to Customer, the following terms shall apply unless otherwise specified in an Order:

- a. Unless **Supplier** Equipment is purchased by Customer, Xerox (or the applicable third party vendor) shall at all times retain title to the Supplier Equipment. Customer hereby authorizes Xerox or its agents to file financing statements necessary to protect Xerox's rights to Supplier Equipment. Each party will promptly notify the other, in writing, of any change in ownership, or if it relocates its principal place of business, or changes the name of its business. The risk of loss for the Supplier Equipment shall pass to Customer upon delivery to the applicable Customer Facilities. Customer will insure the Supplier Equipment against loss or damage and the policy will name Xerox as loss payee.
- b. Customer agrees to use the Supplier Equipment in accordance with, and to perform, all operator maintenance procedures for the Supplier Equipment described in the applicable Documentation made available or provided by Xerox. The Customer shall not (unless the Supplier Equipment is Purchased Equipment, and then only with Xerox's prior consent):
 - i. sell, charge, let or part with possession of the Supplier Equipment;
 - ii. remove the Supplier Equipment from Customer Facilities in which it is installed; or
 - iii. make any changes or additions to the Supplier Equipment.
- c. **Early Termination.** Equipment is provided for a minimum order term (as specified in the applicable Order per EQP 1.1 above). If Equipment is terminated for any reason before the end of its minimum order term, the termination charges set forth in the applicable Order or Services Contract for such Equipment shall apply.

EQP 1.7 – DATA SECURITY

Certain models of Equipment can be configured to include a variety of data security features. There may be an additional cost associated with certain data security features. The selection, suitability and use of data security features are solely Customer's

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

responsibility. Upon request, Xerox will provide additional information to Customer regarding the security features available for particular Equipment models.

EQP 1.8 – REMOTE SERVICES FOR EQUIPMENT

Certain models of Equipment are supported and serviced using Remote Data Access. Remote Data Access also enables Xerox to transmit to the Customer Maintenance Releases or Updates for software or firmware and to remotely diagnose and modify Equipment to repair or correct malfunctions. Remote Data will be transmitted to and from Customer in a secure manner specified by Xerox. Remote Data Access will not allow Xerox to read, view or download any Customer data, documents or other information residing on or passing through the Equipment, Third Party Hardware or Customer's information management systems. Customer grants the right to Xerox, without charge, to establish and maintain Remote Data Access for the purposes described above. Upon Xerox's request, Customer will provide contact information for Equipment such as name and address of Customer contact and IP and physical addresses/locations of Equipment. Customer will enable Remote Data Access via a method prescribed by Xerox and Customer will provide Xerox with reasonable assistance to allow Xerox to have Remote Data Access. Unless Xerox deems Equipment incapable of Remote Data Access, Customer will ensure that Remote Data Access is maintained at all times Maintenance Services are being performed.

EQP 1.9 - TOTAL SATISFACTION GUARANTEE.

- a. "SP Equipment" means any iGen3, iGen4, iGen150, iGen5 or Xerox Color 8250 Production Printer. If, during any 90 day period, the performance of SP Equipment delivered under this Agreement is not at least substantially consistent with the performance expectations outlined in the SP Equipment's Customer Expectations Document ("Expectations Document"), Xerox will, at Customer's request, replace the SP Equipment without charge with identical SP Equipment or, at Xerox's option, with Equipment with comparable features and capabilities (the "SP Equipment Guarantee"). The SP Equipment Guarantee does not apply during the first 180 days after installation and will expire at the end of the initial term of the Order; provided however, for SP Equipment identified as "Previously Installed", this SP Equipment Guarantee expires 1 year after installation. This SP Equipment Guarantee applies only to SP Equipment that has been (i) continuously maintained by Xerox through the provision of Xerox Maintenance Services, and (ii) operated at all times in accordance with the Expectations Document.
- b. "Non-SP Equipment" means any Equipment other than SP Equipment. If Customer is not completely satisfied with any Non-SP Equipment delivered under an Order under this Agreement, Xerox will, at Customer's request, replace it without charge with identical Non-SP Equipment or, at the option of Xerox, with Equipment with comparable features and capabilities (the "Non-SP Equipment Guarantee"). The Non-SP Equipment Guarantee applies only to Non-SP Equipment that has been continuously maintained by Xerox through the provision of Xerox Maintenance Services. The Non-SP Equipment Guarantee will expire at the end of the initial term of the subject Order; provided however, for Non-SP Equipment identified as "Previously Installed", the Non-SP Equipment Guarantee expires 1 year after the Installation Date. The Non-SP Equipment Guarantee does not apply to a limited number of Non-SP Equipment models, which models are identified in the applicable Order Document.
- c. The SP Equipment Guarantee and Non-SP Equipment Guarantee replace and supersede any other guarantee from Xerox, whether made orally or in writing, styled a "Total Satisfaction Guarantee", "Satisfaction Guarantee" or otherwise covering the subject matter set forth above.

EQP 1.10 – REMOVAL OF HAZARDOUS WASTE

Customer agrees to take responsibility for legally disposing of all hazardous wastes generated from the use of Third Party Hardware or supplies.

EQUIPMENT PURCHASE MODULE

EP 1 – TERMS AND CONDITIONS SPECIFIC TO EQUIPMENT PURCHASE

In addition to the terms and conditions in the General (GEN) Module, the following terms and conditions apply to the acquisition of Purchased Equipment:

EP 1.1 – ORDER

Orders for an outright purchase of Equipment shall include the unique Xerox-provided contract number and the number of this Agreement on all applicable ordering documents.

EP 1.2 – TITLE

Title to Purchased Equipment will pass to Customer upon delivery to the applicable Customer Facilities.

EP 1.3 – DEFAULT

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

If Customer defaults under a XOA for Purchased Equipment, Xerox, in addition to its other remedies (including the cessation of Maintenance Services if applicable), may require immediate payment of all amounts then due, plus all Transaction Taxes and applicable interest on all amounts due from the due date until paid. Customer shall also pay all reasonable costs, including attorney's fees, incurred by Xerox to enforce this Agreement.

EP 1.4 – MAINTENANCE SERVICES FOR PURCHASED EQUIPMENT

If Customer elects to receive Maintenance Services for Purchased Equipment, Customer shall do so under a separate Order under the Agreement for such Maintenance Services.

EP 1.5 – AGREEMENT PROVISION EXCLUSIONS

The following Agreement provisions do not apply to Orders for an outright purchase of Equipment: GEN 1.1 c.ii – iii; GEN 1.6 b – j; GEN 1.7 b.1; GEN 1.11; EQP 1.4; EQP 1.6.

MAINTENANCE SERVICES MODULE

MS 1 – TERMS AND CONDITIONS SPECIFIC TO MAINTENANCE SERVICES

In addition to the terms and conditions in the General (GEN) Module, and except as otherwise set forth in an Order, the following terms and conditions apply to provision of Maintenance Services.

MS 1.1 – MAINTENANCE SERVICES

As part of an Order for (a) stand-alone Maintenance Services related to Purchased Equipment, or (b) Maintenance Services related to Equipment to which Xerox does not hold title, or as a mandatory part of an Order for Equipment (other than Purchased Equipment) that includes Maintenance Services, Xerox or a designated service provider will provide the following Maintenance Services for Equipment. If Customer is acquiring Equipment for which Xerox does not offer Maintenance Services, such Equipment will be designated as "No Svc." This Module does not apply to maintenance of Third Party Hardware. Maintenance that Xerox provides on Third Party Hardware will be provided in accordance with the terms of the applicable Order.

The provision of Maintenance Services is contingent upon Customer facilitating timely and efficient resolution of Equipment issues by: (i) utilizing Customer-implemented remedies provided by Xerox; (ii) replacing Cartridges; and (iii) providing information to and implementing recommendations provided by Xerox telephone support personnel in those instances where Xerox is not providing on-site Equipment support personnel. If an Equipment issue is not resolved after completion of (i) through (iii) above, Xerox will provide on-site support as provided in the applicable Order.

MS 1.2 – REPAIRS AND PARTS

- a. Xerox will make repairs and adjustments necessary to keep the Equipment in good working order and operating in accordance with its written specifications (including such repairs or adjustments required during initial installation). Maintenance Services shall cover repairs and adjustments required as a result of normal wear and tear or defects in materials or workmanship. Parts required for repair may be new, reconditioned, reprocessed or recovered.
- b. If Xerox is providing Maintenance Services for Equipment that uses Cartridges, Customer will use only unmodified Cartridges purchased directly from Xerox or its authorized resellers. Failure to use such Cartridges will void any warranty applicable to such Equipment. Cartridges packed with Equipment or furnished by Xerox as Consumable Supplies will meet Xerox's new Cartridge performance standards and may be new, remanufactured or reprocessed and contain new and/or reprocessed components. To enhance print quality, Cartridges for many models of Equipment have been designed to cease functioning at a predetermined point. Many Equipment models are designed to function only with Cartridges that are newly manufactured original Xerox Cartridges or with Cartridges intended for use in the U.S.

MS 1.3 – HOURS AND EXCLUSIONS

Unless otherwise set forth in an Order, Maintenance Services will be provided in areas accessible for repair services during Xerox's standard working hours. Maintenance Services excludes repairs due to: (a) misuse, neglect or abuse; (b) failure of the installation site or the PC or workstation used with the Equipment to comply with Xerox's published specifications; (c) use of options, accessories, or other products not serviced by Xerox; (d) non-Xerox alterations, relocation, service or supplies; and (e) failure to perform operator maintenance procedures identified in operator manuals. Customer agrees to furnish all referenced parts, tools, and supplies needed to perform those procedures that are described in the applicable manuals and instructions.

MS 1.4 – INSTALLATION SITE AND METER READINGS

In order to receive Maintenance Services for Equipment requiring connection to a PC or workstation, Customer must utilize a PC or workstation that either (a) has been provided by Xerox or (b) meets Xerox's published specifications. The Equipment installation site must conform to Xerox's published requirements. If applicable, unless otherwise set forth in an Order, Customer agrees to provide meter readings in the manner prescribed by Xerox. If Customer does not provide Xerox with meter readings

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

as required, for Equipment not capable of Remote Data Access, or if Remote Data Access is interrupted, Xerox may estimate them and bill Customer accordingly.

MS 1.5- REMEDY

If Xerox is unable to maintain the Equipment as described above, Xerox will, as Customer's exclusive remedy for Xerox's failure to provide Maintenance Services, replace the Equipment with an identical product or, at Xerox's option, another model with comparable features and capabilities. If replacement Equipment is provided pursuant to this Section, there shall be no additional charge for its provision by Xerox during the initial term of the Order and it shall be subject to the terms and conditions of this Agreement and the applicable Order(s). Customer's use of non-Xerox approved consumables that affect the performance of the Equipment may invalidate this remedy.

MS 1.6- END OF SERVICE

Xerox has no obligation to maintain or replace Equipment beyond the "End of Service" for that particular model of Equipment. End of Service ("EOS") means the date announced by Xerox after which Xerox will no longer offer Maintenance Services for a particular Equipment model. An EOS Equipment List is available upon request.

SOFTWARE LICENSE MODULE

SW 1 - TERMS AND CONDITIONS SPECIFIC TO SOFTWARE

In addition to the terms and conditions in the General (GEN) Module the following terms and conditions apply to the license and use of Software and its associated Documentation.

SW 1.1- SOFTWARE LICENSE

Xerox may provide Software to Customer pursuant to an Order hereunder. The following license applies to Software provided hereunder, unless such Software is accompanied by a click-wrap or shrink-wrap license agreement or otherwise provided subject to a separate license agreement.

- a. Xerox grants Customer a non-exclusive, non-transferable, non-assignable (by operation of law or otherwise) license to use in the U.S.: (i) Base Software only on or with the Equipment with which (or within which) it was delivered; and (ii) Application Software only on any single unit of Equipment, subject to Customer remaining current in the payment of any indicated applicable Software license fees (including any annual renewal fees). Customer has no other rights to the Software. Customer will not and will not allow its employees, agents, contractors or vendors to: (i) distribute, copy, modify, create derivatives of, decompile, or reverse engineer Software except as permitted by applicable law; (ii) activate Software delivered with or within the Equipment in an un-activated state; or, (iii) access or disclose Diagnostic Software for any purpose. Title to Software and all copyrights and other intellectual property rights in Software will reside solely with Xerox and its licensors (who will be considered third party beneficiaries of this Agreement's software and limitation of liability provisions).
- b. The Base Software license will terminate: (i) if Customer no longer uses or possesses the Equipment with which the Base Software was provided; or (ii) upon the expiration or termination of any Order under which Customer has acquired the Equipment with which the Base Software was provided (unless Customer has exercised an option to purchase the Equipment, where available).
- c. Software may contain code to prevent its unlicensed use and/or transfer. If you do not permit Xerox periodic access to such Software, this code may impair the Equipment's and/or Software's functionality.
- d. Xerox does not warrant that the Software will be free from errors or that its operation will be uninterrupted.

SW 1.2- SOFTWARE SUPPORT

Software support will be provided by Xerox or a designated service provider as follows. For Base Software, Software support will be provided during the initial term of the applicable Order and any renewal period, but not longer than five (5) years after Xerox stops taking orders for the subject model of Equipment. For Application Software, Software support will be provided as long as Customer is current in the payment of all applicable software license, annual renewal and "support only" fees.

- a. Xerox will maintain a web-based or toll-free hotline during Xerox's standard working hours to report Software problems and answer Software-related questions. Xerox, either directly or with its vendors, will make reasonable efforts to: (i) assure that Software performs in material conformity with its Documentation; (ii) provide available workarounds or patches to resolve Software performance problems; and (iii) resolve coding errors for (1) the current release and (2) the previous release for a period of six (6) months after the current release is made available to Customer. Xerox will not be required to provide Software support if Customer has modified the Software.
- b. Xerox may make available new releases of the Software that are designated as "**Maintenance Releases**" or "**Updates.**" Maintenance Releases or Updates are provided at no charge and must be implemented within six (6)

**Xerox Clarification/Exceptions to
The Regents of the University of California
Request for Proposal #
Print, Goods and Services**

months after being made available to Customer. Each Maintenance Release or Update shall be considered Software governed by these terms. Feature Releases will be subject to additional license fees at Xerox's then-current pricing and shall be considered Software governed by these terms and conditions (unless otherwise noted in an Order). Implementation of a Maintenance Release, Update or Feature Release may require Customer to procure, at its expense, additional hardware and/or software from Xerox or another entity. Upon installation of a Maintenance Release, Update or Feature Release, Customer will return or destroy all prior Maintenance Releases, Updates or Feature Releases.

- c. Xerox may annually increase Software license fees and support fees for Application Software.

SW 1.3- DIAGNOSTIC SOFTWARE

Diagnostic Software and method of entry or access to it constitute valuable trade secrets of Xerox. Title to the Diagnostic Software shall at all times remain solely with Xerox and Xerox's licensors. Xerox does not grant Customer a license or right to use the Diagnostic Software. Customer will not use, reproduce, distribute, or disclose the Diagnostic Software for any purpose (or allow third parties to do so). Customer will allow Xerox reasonable access to the Equipment during Customer's normal business hours to remove or disable Diagnostic Software if Customer is no longer receiving Maintenance Services from Xerox.

SW 1.4 - THIRD PARTY SOFTWARE

Third Party Software is subject to license and support terms provided by the applicable Third Party Software vendor.

IN WITNESS WHEREOF, the parties have executed this Agreement on the dates set forth below intending it to become effective on the Effective Date and thereby agreeing to its terms.

ENTER CUSTOMER NAME

XEROX CORPORATION

Signature

Name (please print)

Title

Address

Date

Signature

Name

Title

Address

Date

END OF CLARIFICATIONS AND ADDITIONAL TERMS

Executive Summary

Xerox is appreciative of the opportunity to respond to this RFP and we understand that in order for UC Systems to succeed, your attention needs to be focused firmly on your core business of education, not on managing print.

As evidenced by the release of your Request for Proposal (RFP), you acknowledge that outsourcing print related activities to a partner is the most effective way to accomplish your objectives. To that end, we have shown ourselves to be a trust-worthy partner of USC for the past 20+ years with a focused effort on high levels of service and support with faculty and staff requirements for print across the campus. We have partnered with Pharos to deliver top tier student print experience at your libraries.

In addition, our proposal will continue to build on our excellent end user support model that has been proven to deliver excellent performance on your campuses:

- We will continue to provide the full-service support model.
- Maintain our tenured and experienced Account Services Engineers whose commitment has helped our technical team exceed SLA performance measurements.
- Sustain high levels of end user satisfaction working closely with IT Services and users on campus.
- Provide efficient billing and accounting within our customer support model
- Drive fast and efficient service (SLA's) and appropriate training and support.
- Ensure all end users are satisfied and all supplies are managed as prescribed by the department.
- Conduct ongoing Quarterly Business Reviews that hold Xerox accountable for all our agreed performance measurements.

Gateway to New Possibilities

Multifunction printers built on Xerox® ConnectKey® Technology are more than machines. They are workplace assistants and the centerpiece of a workplace transformation and productivity ecosystem combining all the technologies, capabilities and extensibility you need to let your work - and work teams - flow.

ConnectKey® Technology brings an entirely new level of flexibility, efficiency and possibility to your workforce with both its native apps and those available through the Xerox® App Gallery.



Native apps simplify print, scan and copy functions, as well as provide access to contact lists and frequently used locations, while apps available through the App Gallery allow users to download serverless apps like Print from Dropbox™ and Scan to Microsoft® Office 365® directly from the user interface.

With Xerox® App Studio and Personalized Application Builder (PAB), Xerox partners can offer even more sophisticated levels of customization to automate your unique workflow requirements.

Benchmark Security

Security is a top priority for every business. Xerox ConnectKey® Technology exceeds industry standards for security features and technologies allowing you to work with total peace of mind.

A Higher Standard – Leader in Print Security (we our FedRamp Certified)

Although it's integral to our technology, there's nothing standard about the levels of security included with every ConnectKey® enabled device. Our holistic four-point approach to security ensures comprehensive and all-encompassing protection for all system components and points of vulnerability.

Intrusion Prevention

ConnectKey® Technology utilizes a comprehensive set of capabilities that prevents malicious attacks, the proliferation of malware, and misuse of/unauthorized access to the printer, whether from transmitted data or direct interaction at the device.

All possible access points are secure, including the user interface and input ports accessible to walkup users as well as PC, server, mobile devices or cloud connections.

Device Detection

Xerox® ConnectKey® Technology runs a comprehensive Firmware Verification test, either at start-up* or when activated by authorized users. This provides alerts if any harmful changes to the printer have been detected. McAfee® Whitelisting** technology constantly monitors for and automatically prevents any malicious malware from running.

Document and Data Protection

Our comprehensive security measures do not stop with preventing unauthorized access to your printer and securing your information from the inside. ConnectKey® Technology provides capabilities to prevent intentional or unintentional transmission of critical data to unauthorized parties.

From protecting printed materials by not releasing documents until the right user is at the device, to preventing scanned information reaching beyond its intended recipient, ConnectKey® Technology offers the safeguards you need to keep your most critical data assets safe and secure.

Xerox also protects all your stored information, using the highest levels of encryption. You can delete any processed or stored data that is no longer required using National Institute of Standards and Technology (NIST), and U.S. Department of Defense approved data clearing and sanitization algorithms.

External Partnerships

ConnectKey® Technology provides extra security standards through our partnership with McAfee®*. We measure our performance against international standards with certifications like Common Criteria and FIPS 140-2 to ensure our devices are trusted in even the most secure environments.

	Intrusion Prevention Safeguard access and data transmission to the device
	Device Detection Verification to alert against harmful changes to system firmware
	Document and Data Protection Lockdown security from unauthorized disclosure of information; secure data on the device
	External Partnerships Highest security standards with McAfee, and industry certifications

Environmental Sustainability

Many of our products meet or exceed the minimum registration requirements for product environmental performance. Along with EPEAT, Xerox offers ENERGY STAR®, ECOLOGO® and Blue Angel certified office products and with its partnership with PrintReleaf, enables managed print services customers to offset their printing by planting trees in endangered geographies.

Thank you for the opportunity to share our proposal. We look forward to the next phases of the procurement process and to continuing our partnership with the University of California.

Reference 1

Organization Name	UC San Diego
Address	9500 Gilman Drive, La Jolla, CA 92093
Telephone Number	858-534-4834
Website Address	https://www.ucsd.edu/indes.html
Contact Person Name	Gina Webb
Title	Interim Manager
Start & End Date of Service	Over 20 years, outright purchase of Xerox equipment --- Xerox equipment, service & supplies
Services Provided	

Reference 2

Organization Name	University of Hawaii at Manoa
Address	2465 Campus Road, Honolulu, HI 96822
Telephone Number	808-956-8365
Website Address	https://manoa.hawaii.edu/
Contact Person Name	Jchang22@hawaii.edu
Title	Campus Solution Manager
Start & End Date of Service	April 1, 2020 to March 31, 2025
Services Provided	Over 100 MFD's, Managed Print, Onsite Labor

Reference 3

Organization Name	University of Pacific
Address	3601 Pacific Avenue, Stockton, CA 95211
Telephone Number	(916) 874-7034
Website Address	
Contact Person Name	Kevin Lemoine
Title	IT Project Manager
Start & End Date of Service	07/01/2010 - Present
Services Provided	UOP solicited a bid requesting one vendor to provide Managed Print Services for MFP and printer fleet. PaperCut software would be included to allow UOP IT staff to track and bill all Staff and Student printing. MFP devices would include card readers. ID badges would authenticate and release print jobs. USB ports were plugged to eliminate the possibility of students using USB to avoid print charges. Bid was awarded to Zoom Imaging Systems in 2010 with Toshiba MFP's. Zoom Imaging was rolled into Inland in 2019, resulting in Inland stepping into management of this account for UOP's 3 campuses: Stockton, Sacramento, and San Francisco.

Reference 4

Organization Name	Napa Valley College
Address	2277 Napa-Vallejo Highway, Napa, CA 94558
Telephone Number	(707) 256-7175
Website Address	
Contact Person Name	Robert Parker
Title	VP Administrative Services
Start & End Date of Service	11/01/2016 – Present
Services Provided	Napa Valley College wanted to continue with Inland as equipment and service provider, but Purchaser felt it was mandated to solicit a bid. A national Co-Op contract was leveraged to avoid the cost & time of preparing a RFP. An Implementation Schedule was developed based on NVC's timeframe. Inland provided an onsite analyst to aid NVC IT staff in network installation. A Master Lease Schedule was created to allow NVC to add Xerox units on campus, as needed. A Print Service Agreement was recently negotiated, reflecting in NVC saving \$12,000 annually. PaperCut will soon be implemented for an additional 15% print savings.

Reference 5

Organization Name	CSU Fullerton
Address	800 N. State College Blvd., Fullerton, CA
Telephone Number	657-278-2413
Website Address	www.fullerton.edu
Contact Person Name	Nelson Nagai
Title	Senior Director, Contracts & Procurement
Start & End Date of Service	5/2017-5/2022
Services Provided	Xerox Managed Services, Xerox equipment, service, supplies, on-site Xerox labor, installation of Xerox equipment onto CSUF network, Xerox Device Management (XDM) tool for proactive monitoring of devices, Quarterly Business Reviews with customized reporting.

Reference 6

Organization Name	UCSF Documents and Media for UCSF and Berkeley
Address	1855 Folsom Street, San Francisco, CA.
Telephone Number	(415) 502-3072
Website Address	Mike.Brower@UCSF.edu
Contact Person Name	Mike Brower or Mario Carmona (Please Contact Xerox Representative: Scott Reiber) mobile: 505-264-7071 Email: scott.reiber@xerox.com
Title	Manager of Documents and Media
Start & End Date of Service	
Services Provided	

Organization Chart

Doug MacPhee, Vice President of Sales, will have overall responsibility for the management of the UC relationship. Additionally, we have a team of 5 regionally based Client Managers who provide localized support to the 10 UC campuses and dozens of California-based internal Xerox resources who support the account team. All of our sales resources are based in California and located within close proximity to the UC campuses they support. The UC's first escalation point is to the client manager listed below. If an item needs to be escalated beyond the client manager, Jim Potts is the appropriate management resource for resolution/escalation.

Organization Chart for Xerox UC support team:



Escalation Process and Chain of Command for Problem Resolution

Area	Level One		Level Two		Level Three	
	Why / When to Call	Who to Call	Why / When to Call	Who to Call	Why / When to Call	Who to Call
Customer Issues	Customer issues	Xerox Customer Service Unit	Customer issues beyond the control of or not resolved by Customer Service	Client Manager	Customer issues beyond the control of or not resolved by Client Manager	Account General Manager
Sales	Requests for Sales related issues or support	Xerox Customer Service Unit	Requests for Sales related issues or support not being addressed by Customer Service	Client Manager	Requests for Sales related issues or support not being addressed by Client Manager	Public Sector Sales Manager
Technical Service	Routine Service required	Xerox Service Help Desk	Technical Service issues not resolved in a timely fashion by Help Desk/Customer Service Engineer	Area Service Manager	Technical Service issues not resolved in a timely fashion by Area Service Manager	VP Technical Services

Technical Service Escalation/Problem Resolution Process

The steps for problem escalation are as follows:

- **If the problem is not identified:** Customer Service Engineer (CSE) contacts the Xerox Hotline to notify the Work Group Leader, who must respond within one hour.
- **If the problem remains unidentified and or unresolved:** CSE re-contacts the Work Group Leader and the Xerox Field Manager for Customer Service to get further assistance and direction. This activity must transpire within 1-3 hours.
- **If Problem is still not identified or resolved:** CSE contacts Work Group Leader, Customer Service Technical Specialist, and Field Manager for Customer Service to obtain further suggestions/information. This should occur within 3-4 hours.
- **If Problem is still not identified or resolved:** CSE makes arrangements to receive site assistance from Work Group Leader/Customer Service Technical Specialist and notifies the customer's decision maker on equipment status. This should occur within four to six hours.
- **If Problem is still not identified or resolved:** CSE, Work Group Leader and Customer Service Technical Specialist contact Field Manager Technical Service to seek assistance outside the immediate support team. This should occur within six to eight hours.
- **If Xerox is unable to correct the issue at this point:** Customer can be assured that they may invoke the "Total Satisfaction Guarantee" clause in the contract.

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K

CURRENT REPORT

Pursuant to Section 13 or 15(d) of
the Securities Exchange Act of 1934

Date of Report (date of earliest event reported): January 28, 2020

xerox[™]

XEROX HOLDINGS CORPORATION
XEROX CORPORATION

(Exact Name of Registrant as specified in its charter)

New York
New York

(State or other jurisdiction of incorporation or organization)

001-39013
001-04471

(Commission File Number)

83-3933743
16-0468020

(IRS Employer
Identification No.)

201 Merritt 7
Norwalk, Connecticut
06851-1056

(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code: (203) 968-3000

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol	Name of each exchange on which registered
Xerox Holdings Corporation Common Stock, \$1 par value	XRX	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act:

None

Indicate by check mark whether the Registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§ 230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company

If an emerging growth company, indicate by check mark if the Registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

Item 2.02. Results of Operations and Financial Condition.

On January 28, 2020, Registrant released its fourth quarter 2019 earnings and is furnishing to the Securities and Exchange Commission ("SEC") a copy of the earnings press release as Exhibit 99.1 to this Report under Item 2.02 of Form 8-K.

Exhibit 99.1 to this Report contains certain financial measures that are considered "non-GAAP financial measures" as defined in the SEC rules. Exhibit 99.1 to this Report also contains the reconciliation of these non-GAAP financial measures to their most directly comparable financial measures calculated and presented in accordance with generally accepted accounting principles, as well as the reasons why Registrant's management believes that presentation of the non-GAAP financial measures provides useful information to investors regarding Registrant's results of operations and, to the extent material, a statement disclosing any other additional purposes for which Registrant's management uses the non-GAAP financial measures.

The information contained in Item 2.02 of this Report and in Exhibit 99.1 to this Report shall not be deemed "filed" with the Commission for purposes of Section 18 of the Exchange Act of 1934, as amended, or otherwise subject to the liability of that section.

Item 9.01. Financial Statements and Exhibits.

(d) Exhibits.

Exhibit No.	Description
<u>99.1</u>	Registrant's fourth quarter 2019 earnings press release dated January 28, 2020

Forward-Looking Statements

This filing, and other written or oral statements made from time to time by management contain "forward-looking statements" as defined in the Private Securities Litigation Reform Act of 1995. The words "anticipate", "believe", "estimate", "expect", "intend", "will", "should", "targeting", "projecting", "driving" and similar expressions, as they relate to us, our performance and/or our technology, are intended to identify forward-looking statements. These statements reflect management's current beliefs, assumptions and expectations and are subject to a number of factors that may cause actual results to differ materially. Such factors include but are not limited to: our ability to address our business challenges in order to reverse revenue declines, reduce costs and increase productivity so that we can invest in and grow our business; our ability to attract and retain key personnel; changes in economic and political conditions, trade protection measures, licensing requirements and tax laws in the United States and in the foreign countries in which we do business; the imposition of new or incremental trade protection measures such as tariffs and import or export restrictions; changes in foreign currency exchange rates; our ability to successfully develop new products, technologies and service offerings and to protect our intellectual property rights; the risk that multi-year contracts with governmental entities could be terminated prior to the end of the contract term and that civil or criminal penalties and administrative sanctions could be imposed on us if we fail to comply with the terms of such contracts and applicable law; the risk that partners, subcontractors and software vendors will not perform in a timely, quality manner; actions of competitors and our ability to promptly and effectively react to changing technologies and customer expectations; our ability to obtain adequate pricing for our products and services and to maintain and improve cost efficiency of operations, including savings from restructuring actions; the risk that confidential and/or individually identifiable information of ours, our customers, clients and employees could be inadvertently disclosed or disclosed as a result of a breach of our security systems due to cyber attacks or other intentional acts; reliance on third parties, including subcontractors, for manufacturing of products and provision of services; the exit of the United Kingdom from the European Union; our ability to manage changes in the printing environment and expand equipment placements; interest rates, cost of borrowing and access to credit markets; funding requirements associated with our employee pension and retiree health benefit plans; the risk that our operations and products may not comply with applicable worldwide regulatory requirements, particularly environmental regulations and directives and anti-corruption laws; the outcome of litigation and regulatory proceedings to which we may be a party; any impacts resulting from the restructuring of our relationship with Fujifilm Holdings Corporation; the shared services arrangements entered into by us as part of Project Own It; the ultimate outcome of any possible transaction between Xerox Holdings Corporation ("Xerox") and HP Inc. ("HP"), including the possibility that the parties will not agree to pursue a business combination transaction or that the terms of any definitive agreement will be materially different from those proposed; uncertainties as to whether HP will cooperate with Xerox regarding the proposed transaction; the ultimate result should Xerox determine to commence a proxy contest for election of directors to HP's board of directors; Xerox's ability to consummate the proposed transaction with HP; the conditions to the completion of the proposed transaction, including the receipt of any required shareholder approvals and any required regulatory approvals; Xerox's ability to finance the proposed transaction with HP; Xerox's indebtedness, including the substantial indebtedness Xerox expects to incur in connection with the proposed transaction with HP and the need to generate sufficient cash flows to service and repay such debt; the possibility that Xerox may be unable to achieve expected synergies and operating efficiencies within the expected time-frames or at all and to successfully integrate HP's operations with those of Xerox; that such integration may be more difficult, time-consuming or costly than expected; that operating costs, customer loss and business disruption (including, without limitation, difficulties in maintaining relationships with employees, customers or suppliers) may be greater than expected following the proposed transaction or the public announcement of the proposed transaction; the retention of certain key employees may be difficult; and general economic conditions that are less favorable than expected. Additional risks that may affect Xerox's operations and other factors that are set forth in the "Risk Factors" section, the "Legal Proceedings" section, the "Management's Discussion and Analysis of Financial Condition and Results of Operations" section and other sections of Xerox Corporation's 2018 Annual Report on Form 10-K, as well as in Xerox Corporation's and Xerox Holdings Corporation's Quarterly Reports on Form 10-Q and Current Reports on Form 8-K filed with the SEC. These forward-looking statements speak only as of the date of this filing or as of the date to which they refer, and Xerox assumes no obligation to update any forward-looking statements as a result of new information or future events or developments, except as required by law.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, each registrant has duly caused this report to be signed on its behalf by the undersigned thereunto duly authorized. The signatures for each undersigned shall be deemed to relate only to matters having reference to such company and its subsidiaries.

XEROX HOLDINGS CORPORATION

(Registrant)

By: /S/ JOSEPH H. MANCINI, JR.

Joseph H. Mancini, Jr.
Vice President and
Chief Accounting Officer
(Principal Accounting Officer)

Date: January 28, 2020

XEROX CORPORATION

(Registrant)

By: /S/ JOSEPH H. MANCINI, JR.

Joseph H. Mancini, Jr.
Vice President and
Chief Accounting Officer
(Principal Accounting Officer)

Date: January 28, 2020

EXHIBIT INDEX

Exhibit No.	Description
99.1	Registrant's fourth quarter 2019 earnings press release dated January 28, 2020
101	Cover Page Interactive Data File - the cover page XBRL tags are embedded within the Inline XBRL document.
104	The cover page from this Current Report on Form 8-K, formatted as Inline XBRL.

News from Xerox Holdings Corporation



For Immediate Release

Xerox Holdings Corporation
201 Merritt 7
Norwalk, CT 06851-1056
tel+1-203-968-3000

Xerox Exceeds Q4 EPS Guidance, Delivers Strong Cash Flow and Operating Margin

Announces 2020 guidance consistent with three-year plan, including further EPS expansion and revenue trend improvement

2019 Full-Year Financial Highlights:

- GAAP earnings per share (EPS) from continuing operations of \$2.78, up \$1.62 year-over-year (YOY); adjusted EPS from continuing operations of \$3.55, up \$0.67 YOY.
- Adjusted operating margin of 13.1 percent, up 180 basis points YOY.
- \$1.24 billion of operating cash flow from continuing operations, up \$162 million YOY; \$1.18 billion of free cash flow, up \$187 million YOY.
- \$9.07 billion of revenue, a decrease of 6.2 percent in actual currency YOY or 4.7 percent in constant currency YOY.
- Achieved gross savings of \$640 million under Project Own It, Xerox's enterprise-wide initiative to simplify operations, drive continuous improvement and free up capital to reinvest in the business.
- Returned 72 percent of free cash flow to shareholders.

NORWALK, Conn., Jan. 28, 2020 - Xerox Holdings Corporation (NYSE: XRX) announced its fourth-quarter and full-year 2019 financial results and 2020 guidance.

"We are delivering on our three-year plan. We grew earnings per share, increased cash flow and expanded adjusted operating margin for the full year, and we improved our revenue trajectory in the second half of the year as our investments in the business gained traction," said Xerox Vice Chairman and CEO John Visentin. "We accomplished this while returning more than 70 percent of free cash flow to shareholders, paying down approximately \$950 million in debt and increasing investments in our innovation areas. We are well-positioned to carry this momentum into 2020 and lead the way for long-overdue industry consolidation."

Fourth-Quarter Key Financial Results - Continuing Operations:

(in millions, except per share data)	Q4 2019	Q4 2018	B/(W) YOY	% Change YOY
Revenue	\$2,444	\$2,498	\$(54)	(2.2)% AC (1.6)% CC¹
Gross Margin	41.6%	40.0%	160 bps	
RD&E %	3.8%	3.8%	—	
SAG %	20.9%	22.1%	120 bps	
Pre-Tax Income	\$336	\$124	\$212	171.0%
Pre-Tax Income Margin	13.7%	5.0%		
Operating Income - Adjusted¹	\$411	\$352	\$59	16.8%
Operating Margin - Adjusted ¹	16.8%	14.1%	270 bps	
GAAP EPS	\$1.17	\$0.37	\$0.80	216.2%
EPS - Adjusted¹	\$1.33	\$0.94	\$0.39	41.5%

Full-Year Key Financial Results - Continuing Operations:

(in millions, except per share data)	2019	2018	B/(W) YOY	% Change YOY
Revenue	\$9,066	\$9,662	\$(596)	(6.2)% AC (4.7)% CC¹
Gross Margin	40.3%	40.0%	30 bps	
RD&E %	4.1%	4.1%	0	
SAG %	23.0%	24.6%	160 bps	
Pre-Tax Income	\$822	\$549	\$273	49.7%
Pre-Tax Income Margin	9.1%	5.7%		
Operating Income - Adjusted ¹	\$1,192	\$1,093	\$99	9.1%
Operating Margin - Adjusted ¹	13.1%	11.3%	180 bps	
GAAP EPS	\$2.78	\$1.16	\$1.62	139.7%
EPS - Adjusted¹	\$3.55	\$2.88	\$0.67	23.3%

(1) Refer to the "Non-GAAP Financial Measures" section of this release for a discussion of these non-GAAP measures and their reconciliation to the reported GAAP measures.

Fourth-quarter and full-year 2019 results include the benefit from \$77 million of revenue associated with an OEM license agreement with Fuji Xerox received as part of a series of transactions with FUJIFILM Holdings Corporation (FUJIFILM). This benefit was included in Xerox's updated 2019 guidance measures filed with the U.S. Securities and Exchange Commission on Form 8-K on December 3, 2019 that reflected adjustments resulting from the transactions with FUJIFILM.

Full-Year Key Business Highlights:

- Implemented a new supply chain and supplier strategy, which included expanding Xerox's relationship with HP and favorably structuring terms with FUJIFILM that monetized the company's investment in Fuji Xerox at over 20 times 2019 expected aggregate cash flow.
- Expanded Xerox's services portfolio with the launch of Intelligent Workplace Services; IT Services for the small and mid-size business market in the U.S.; and vertical services targeting healthcare, retail, insurance, and the public sector.

- Invested in several industry firsts within Xerox's core technology business such as the **Iridesse® Production Press, Baltoro™ HF Inkjet Press** and **Adaptive CMYK Plus Technology**.
- Made progress on our three-year innovation roadmap with products for 3D printing and AI Workflow Assistants becoming commercially available in 2020 and monetizing innovations through partners.
- Added and renewed several Fortune 500 and public sector clients such as Morgan Stanley, Office Depot, Generali, BAE Systems, the Commonwealth of Massachusetts, the Texas Department of Information Resources and the California Department of State Hospitals.

2020 Guidance:

The company expects continued progress on its strategic initiatives, as projected in its 2020 financial guidance:

- Revenue decline of approximately 4 percent at constant currency, excluding revenue from the \$77 million OEM license in 2019.²
- Adjusted operating margin of approximately 13 percent.
- GAAP EPS from continuing operations in the range of \$2.80 to \$2.90.
- Adjusted EPS in the range of \$3.60 to \$3.70.
- Operating cash flow from continuing operations of approximately \$1.3 billion and free cash flow of approximately \$1.2 billion.
- Company expects at least \$300 million of share repurchases and return of at least 50 percent of annual free cash flow to shareholders in 2020.

(2) Revenue decline of approximately 4.9 percent including the \$77 million OEM License in 2019 .

About Xerox

Xerox Holdings Corporation (NYSE: XRX) makes every day work better. We are a workplace technology company building and integrating software and hardware for enterprises large and small. As customers seek to manage information across digital and physical platforms, Xerox delivers a seamless, secure and sustainable experience. Whether inventing the copier, the ethernet, the laser printer or more, Xerox has long defined the modern work experience. Learn how that innovation continues at xerox.com.

Non-GAAP Measures

This release refers to the following non-GAAP financial measures for the Fourth Quarter and Full-Year 2019 and Full-Year 2020 guidance:

- Adjusted EPS, which excludes restructuring and related costs, the amortization of intangible assets, non-service retirement-related costs, transaction and related costs, net and other discrete adjustments from GAAP-EPS from continuing operations.
- Adjusted operating margin and income, which exclude the EPS adjustments noted above as well as the remainder of other expenses, net from pre-tax margin and income.
- Constant currency (CC) revenue change, which excludes the effects of currency translation.
- Free cash flow, which is cash flow from continuing operations less capital expenditures.

Refer to the "Non-GAAP Financial Measures" section of this release for a discussion of these non-GAAP measures and their reconciliation to the reported GAAP measures.

Forward-Looking Statements

This release, and other written or oral statements made from time to time by management contain "forward-looking statements" as defined in the Private Securities Litigation Reform Act of 1995. The words "anticipate", "believe", "estimate", "expect", "intend", "will", "should", "targeting", "projecting", "driving" and similar expressions, as they relate to us, our performance and/or our technology, are intended to identify forward-looking statements. These statements reflect management's current beliefs, assumptions and expectations and are subject to a number of factors that may cause actual results to differ materially. Such factors include but are not limited to: our ability to address our business challenges in order to reverse revenue declines, reduce costs and increase productivity so that we can invest in and grow our business; our ability to attract and retain key personnel; changes in economic and political conditions, trade protection measures, licensing requirements and tax laws in the United States and in the foreign countries in which we do business; the imposition of new or incremental trade protection measures such as tariffs and import or export restrictions; changes in foreign currency exchange rates; our ability to successfully develop new products, technologies and service offerings and to protect our intellectual property rights; the risk that multi-year contracts with governmental entities could be terminated prior to the end of the contract term and that civil or criminal penalties and administrative sanctions could be imposed on us if we fail to comply with the terms of such contracts and applicable law; the risk that partners, subcontractors and software vendors will not perform in a timely, quality manner; actions of competitors and our ability to promptly and effectively react to changing technologies and customer expectations; our ability to obtain adequate pricing for our products and services and to maintain and improve cost efficiency of operations, including savings from restructuring actions; the risk that confidential and/or individually identifiable information of ours, our customers, clients and employees could be inadvertently disclosed or disclosed as a result of a breach of our security systems due to cyber attacks or other intentional acts; reliance on third parties, including subcontractors, for manufacturing of products and provision of services; the exit of the United Kingdom from the European Union; our ability to manage changes in the printing environment and expand equipment placements; interest rates, cost of borrowing and access to credit markets; funding requirements associated with our employee pension and retiree health benefit plans; the risk that our operations and products may not comply with applicable worldwide regulatory requirements, particularly environmental regulations and directives and anti-corruption laws; the outcome of litigation and regulatory proceedings to which we may be a party; any impacts resulting from the restructuring of our relationship with Fujifilm Holdings Corporation; the shared services arrangements entered into by us as part of Project Own It; the ultimate outcome of any possible transaction between Xerox Holdings Corporation ("Xerox") and HP Inc. ("HP"), including the possibility that the parties will not agree to pursue a business combination transaction or that the terms of any definitive agreement will be materially different from those proposed; uncertainties as to whether HP will cooperate with Xerox regarding the proposed transaction; the ultimate result should Xerox determine to commence a proxy contest for election of directors to HP's board of directors; Xerox's ability to consummate the proposed transaction with HP; the conditions to the completion of the proposed transaction, including the receipt of any required shareholder approvals and any required regulatory a

approvals; Xerox's ability to finance the proposed transaction with HP; Xerox's indebtedness, including the substantial indebtedness Xerox expects to incur in connection with the proposed transaction with HP and the need to generate sufficient cash flows to service and repay such debt; the possibility that Xerox may be unable to achieve expected synergies and operating efficiencies within the expected time-frames or at all and to successfully integrate HP's operations with those of Xerox; that such integration may be more difficult, time-consuming or costly than expected; that operating costs, customer loss and business disruption (including, without limitation, difficulties in maintaining relationships with employees, customers or suppliers) may be greater than expected following the proposed transaction or the public announcement of the proposed transaction; the retention of certain key employees may be difficult; and general economic conditions that are less favorable than expected. Additional risks that may affect Xerox's operations and other factors that are set forth in the "Risk Factors" section, the "Legal Proceedings" section, the "Management's Discussion and Analysis of Financial Condition and Results of Operations" section and other sections of Xerox Corporation's 2018 Annual Report on Form 10-K, as well as in Xerox Corporation's and Xerox Holdings Corporation's Quarterly Reports on Form 10-Q and Current Reports on Form 8-K filed with the SEC. These forward-looking statements speak only as of the date of this release or as of the date to which they refer, and Xerox assumes no obligation to update any forward-looking statements as a result of new information or future events or developments, except as required by law.

-XXX-

Media Contact:

Caroline Gransee-Linsey, Xerox, +1-203-849-2359, Caroline.Gransee-Linsey@xerox.com

Investor Contact:

Ann Pettrone, Xerox, +1-203-849-2590, Ann.Pettrone@xerox.com

Note: To receive RSS news feeds, visit <https://www.news.xerox.com>. For open commentary, industry perspectives and views, visit <http://twitter.com/xerox>, <http://www.facebook.com/XeroxCorp>, <https://www.instagram.com/xerox/>, <http://www.linkedin.com/company/xerox>, <http://www.youtube.com/XeroxCorp>.

Xerox®, Iridesse®, and Baltoro™ are trademarks of Xerox in the United States and/or other countries.

XEROX HOLDINGS CORPORATION
CONDENSED CONSOLIDATED STATEMENTS OF INCOME (UNAUDITED)

(in millions, except per-share data)	Three Months Ended December 31,		Year Ended December 31,	
	2019	2018	2019	2018
Revenues				
Sales ⁽¹⁾	\$ 919	\$ 958	\$ 3,227	\$ 3,454
Services, maintenance and rentals ⁽¹⁾	1,465	1,476	5,595	5,940
Financing	60	64	244	268
Total Revenues	2,444	2,498	9,066	9,662
Costs and Expenses				
Cost of sales ⁽¹⁾	605	613	2,097	2,188
Cost of services, maintenance and rentals ⁽¹⁾	790	855	3,188	3,473
Cost of financing	33	32	131	132
Research, development and engineering expenses	93	94	373	397
Selling, administrative and general expenses	512	552	2,085	2,379
Restructuring and related costs	53	67	229	157
Amortization of intangible assets	10	12	45	48
Transaction and related costs, net	4	5	12	68
Other expenses, net	8	144	84	271
Total Costs and Expenses	2,108	2,374	8,244	9,113
Income before Income Taxes & Equity Income⁽²⁾	336	124	822	549
Income tax expense	73	34	179	247
Equity in net income of unconsolidated affiliates	3	2	8	8
Income from Continuing Operations	266	92	651	310
Income from discontinued operations, net of tax	553	49	710	64
Net Income	819	141	1,361	374
Less: Income from continuing operations attributable to noncontrolling interests	—	1	3	4
Less: Income from discontinued operations attributable to noncontrolling interests	1	3	5	9
Net Income Attributable to Xerox Holdings	\$ 818	\$ 137	\$ 1,353	\$ 361
Amounts Attributable to Xerox Holdings:				
Income from continuing operations	\$ 266	\$ 91	\$ 648	\$ 306
Income from discontinued operations	552	46	705	55
Net Income Attributable to Xerox Holdings	\$ 818	\$ 137	\$ 1,353	\$ 361
Basic Earnings per Share:				
Continuing operations	\$ 1.22	\$ 0.37	\$ 2.86	\$ 1.17
Discontinued operations	2.56	0.19	3.17	0.23
Basic Earnings per Share	\$ 3.78	\$ 0.56	\$ 6.03	\$ 1.40
Diluted Earnings per Share:				
Continuing operations	\$ 1.17	\$ 0.37	\$ 2.78	\$ 1.16
Discontinued operations	2.44	0.19	3.02	0.22
Diluted Earnings per Share	\$ 3.61	\$ 0.56	\$ 5.80	\$ 1.38

⁽¹⁾ Certain prior year amounts have been conformed to the current year presentation. See Appendix III for this change in presentation.

⁽²⁾ Referred to as "Pre-Tax Income" throughout the remainder of this document.

XEROX HOLDINGS CORPORATION
CONDENSED CONSOLIDATED STATEMENTS OF COMPREHENSIVE INCOME (UNAUDITED)

(in millions)	Three Months Ended December 31,		Year Ended December 31,	
	2019	2018	2019	2018
Net income	\$ 819	\$ 141	\$ 1,361	\$ 374
Less: Net income attributable to noncontrolling interests ⁽¹⁾	1	4	8	13
Net Income Attributable to Xerox Holdings	818	137	1,353	361
Other Comprehensive Income (Loss), Net				
Translation adjustments, net	184	(83)	62	(242)
Unrealized (losses) gains, net	(9)	11	(6)	16
Changes in defined benefit plans, net	37	218	(1)	409
Other Comprehensive Income, Net	212	146	55	183
Less: Other comprehensive loss, net attributable to noncontrolling interests ⁽¹⁾	(1)	—	—	—
Other Comprehensive Income, Net Attributable to Xerox Holdings	213	146	55	183
Comprehensive Income, Net	1,031	287	1,416	557
Less: Comprehensive income from continuing operations, net attributable to noncontrolling interests ⁽¹⁾	—	4	8	13
Comprehensive Income, Net Attributable to Xerox Holdings	\$ 1,031	\$ 283	\$ 1,408	\$ 544

⁽¹⁾ Includes continuing and discontinued operations.

XEROX HOLDINGS CORPORATION
CONDENSED CONSOLIDATED BALANCE SHEETS (UNAUDITED)

(in millions, except share data in thousands)	December 31, 2019	December 31, 2018
Assets		
Cash and cash equivalents	\$ 2,740	\$ 1,081
Accounts receivable, net	1,236	1,270
Billed portion of finance receivables, net	111	105
Finance receivables, net	1,158	1,218
Inventories	694	829
Assets of discontinued operations	—	19
Other current assets	201	191
Total current assets	6,140	4,713
Finance receivables due after one year, net	2,082	2,149
Equipment on operating leases, net	364	442
Land, buildings and equipment, net	426	498
Intangible assets, net	199	220
Goodwill	3,900	3,858
Deferred tax assets	596	740
Assets of discontinued operations	—	1,352
Other long-term assets	1,349	902
Total Assets	\$ 15,056	\$ 14,874
Liabilities and Equity		
Short-term debt and current portion of long-term debt	\$ 1,049	\$ 961
Accounts payable	1,053	1,073
Accrued compensation and benefits costs	349	348
Liabilities of discontinued operations	—	21
Accrued expenses and other current liabilities	984	848
Total current liabilities	3,435	3,251
Long-term debt	3,233	4,269
Pension and other benefit liabilities	1,707	1,482
Post-retirement medical benefits	352	350
Other long-term liabilities	512	269
Total Liabilities	9,239	9,621
Convertible Preferred Stock		
	214	214
Common Equity		
Common stock	215	232
Additional paid-in capital	2,782	3,321
Treasury stock, at cost	(76)	(55)
Retained earnings	6,312	5,072
Accumulated other comprehensive loss	(3,637)	(3,565)
Xerox Holdings shareholders' equity	5,596	5,005
Noncontrolling interests	7	34
Total Equity	5,603	5,039
Total Liabilities and Equity	\$ 15,056	\$ 14,874
Shares of common stock issued	214,621	231,690
Treasury stock	(2,031)	(2,067)
Shares of Common Stock Outstanding	212,590	229,623

XEROX HOLDINGS CORPORATION
CONDENSED CONSOLIDATED STATEMENTS OF CASH FLOWS (UNAUDITED)

(in millions)	Three Months Ended December 31,		Year Ended December 31,	
	2019	2018	2019	2018
Cash Flows from Operating Activities				
Net Income	\$ 819	\$ 141	\$ 1,361	\$ 374
Income from discontinued operations, net of tax	(553)	(49)	(710)	(64)
Income from continuing operations	266	92	651	310
Adjustments required to reconcile Net income to Cash flows from operating activities				
Depreciation and amortization	98	128	430	526
Provisions	15	14	73	70
Net gain on sales of businesses and assets	(1)	—	(21)	(35)
Stock-based compensation	9	13	50	57
Restructuring and asset impairment charges	47	66	127	156
Payments for restructurings	(22)	(39)	(93)	(169)
Defined benefit pension cost	20	86	109	175
Contributions to defined benefit pension plans	(34)	(33)	(141)	(144)
(Increase) decrease in accounts receivable and billed portion of finance receivables	(50)	(8)	10	31
Decrease in inventories	78	126	109	17
Increase in equipment on operating leases	(40)	(66)	(153)	(248)
(Increase) decrease in finance receivables	(23)	(15)	101	166
(Increase) decrease in other current and long-term assets	(15)	12	(14)	29
(Decrease) increase in accounts payable	(23)	(27)	(47)	1
Increase (decrease) in accrued compensation	5	(15)	(94)	(111)
Increase in other current and long-term liabilities	21	40	40	52
Net change in income tax assets and liabilities	60	11	90	176
Net change in derivative assets and liabilities	(4)	(12)	11	(14)
Other operating, net	(9)	11	6	37
Net cash provided by operating activities of continuing operations	398	384	1,244	1,082
Net cash provided by operating activities of discontinued operations	40	31	89	58
Net cash provided by operating activities	438	415	1,333	1,140
Cash Flows from Investing Activities				
Cost of additions to land, buildings, equipment and software	(17)	(17)	(65)	(90)
Proceeds from sales of businesses and assets	—	27	21	59
Acquisitions, net of cash acquired	—	—	(42)	—
Other investing, net	—	1	1	2
Net cash (used in) provided by investing activities of continuing operations	(17)	11	(85)	(29)
Net cash provided by investing activities of discontinued operations	2,233	—	2,233	—
Net cash provided by (used in) investing activities	2,216	11	2,148	(29)
Cash Flows from Financing Activities				
Net payments on debt	(551)	(1)	(950)	(307)
Dividends	(60)	(65)	(243)	(269)
Payments to acquire treasury stock, including fees	(232)	(416)	(600)	(700)
Other financing, net	(8)	(3)	(31)	(15)
Net cash used in financing activities of continuing operations	(851)	(485)	(1,824)	(1,291)
Net cash used in financing activities of discontinued operations	—	(1)	(10)	(10)
Net cash used in financing activities	(851)	(486)	(1,834)	(1,301)
Effect of exchange rate changes on cash, cash equivalents and restricted cash	13	(10)	—	(30)
Increase (decrease) in cash, cash equivalents and restricted cash	1,816	(70)	1,647	(220)
Cash, cash equivalents and restricted cash at beginning of period	979	1,218	1,148	1,368
Cash, Cash Equivalents and Restricted Cash at End of Period⁽¹⁾	\$ 2,795	\$ 1,148	\$ 2,795	\$ 1,148

⁽¹⁾ Balance at December 31, 2018 includes \$3 million associated with discontinued operations.

Sales of Ownership Interests in Fuji Xerox Co., Ltd. and Xerox International Partners

In November 2019, Xerox Holdings completed a series of transactions to restructure its relationship with FUJIFILM Holdings Corporation ("FH"), including the sale of its indirect 25% equity interest in Fuji Xerox ("FX") for approximately \$2.2 billion as well as the sale of its indirect 51% partnership interest in Xerox International Partners (XIP) for approximately \$23 million (collectively the "Sales").

As a result of the Sales and the related strategic shift in our business, the historical financial results of our equity method investment in FX and our XIP business, which was fully consolidated, are reflected as a discontinued operation for the periods prior to the Sales, and their impact is excluded from continuing operations for all periods presented.

The transactions with FH also included an OEM license agreement by and between FX and Xerox, granting FX the right to use specific Xerox Intellectual Property (IP) in providing certain named original equipment manufacturers (OEM's) with products (such as printer engines) in exchange for an upfront license fee of \$77 million. The license fee is recorded within other revenues. In addition, arrangements with FX whereby we purchase inventory from and sell inventory to FX, will continue post the Sales and, as a result of our Technology Agreement with Fuji Xerox which remains in effect through March 2021, we will continue to receive royalty payments for FX's use of our Xerox brand trademark, as well as rights to access our patent portfolio in exchange for access to their patent portfolio.

See the "Discontinued Operations" section for additional information. The \$77 million (\$58 million after-tax) OEM license had the following impact on our financial results for the Fourth Quarter 2019 and Full Year 2019:

(in millions, except per share amounts)	Three Months Ended December 31, 2019			Year Ended December 31, 2019		
	As Reported	OEM License Impact	As Reported Excluding OEM License Impact	As Reported	OEM License Impact	As Reported Excluding OEM License Impact
Financial Results from Continuing Operations						
Revenue	(2.2)%	3.1%	(5.2)%	(6.2)%	0.8%	(7.0)%
Revenue - CC ⁽¹⁾	(1.6)%	3.1%	(4.7)%	(4.7)%	0.8%	(5.5)%
Gross Margin	41.6 %	1.9%	39.7 %	40.3 %	0.6%	39.7 %
Adjusted Operating Margin ⁽¹⁾	16.8 %	2.7%	14.1 %	13.1 %	0.7%	12.4 %
EPS - GAAP	\$ 1.17	\$ 0.25	\$ 0.92	\$ 2.78	\$ 0.25	\$ 2.53
EPS - Adjusted ⁽¹⁾	\$ 1.33	\$ 0.25	\$ 1.08	\$ 3.55	\$ 0.25	\$ 3.30
Operating Cash Flow ⁽²⁾	\$ 398	\$ 58	\$ 340	\$ 1,244	\$ 58	\$ 1,186

CC - Constant Currency.

⁽¹⁾ Adjusted measures and CC: see the "Non-GAAP Financial Measures" section for an explanation of the non-GAAP financial measures.

⁽²⁾ Free cash flow likewise impacted by \$58 million from OEM license.

Revenues

(in millions)	Three Months Ended December 31,				% of Total Revenue	
	2019	2018	% Change	CC % Change	2019	2018
Equipment sales	\$ 616	\$ 629	(2.1)%	(1.5)%	25%	25%
Post sale revenue	1,828	1,869	(2.2)%	(1.7)%	75%	75%
Total Revenue	\$ 2,444	\$ 2,498	(2.2)%	(1.6)%	100%	100%
Reconciliation to Condensed Consolidated Statements of Income:						
Sales ⁽¹⁾	\$ 919	\$ 958	(4.1)%	(3.5)%		
Less: Supplies, paper and other sales ⁽¹⁾	(303)	(329)	(7.9)%	(7.3)%		
Equipment Sales	\$ 616	\$ 629	(2.1)%	(1.5)%		
Services, maintenance and rentals ⁽¹⁾	\$ 1,465	\$ 1,476	(0.7)%	(0.2)%		
Add: Supplies, paper and other sales ⁽¹⁾	303	329	(7.9)%	(7.3)%		
Add: Financing	60	64	(6.3)%	(5.9)%		
Post Sale Revenue	\$ 1,828	\$ 1,869	(2.2)%	(1.7)%		
Americas	\$ 1,562	\$ 1,617	(3.4)%	(3.3)%	64%	65%
EMEA	756	830	(8.9)%	(7.4)%	31%	33%
Other	126	51	nm	nm	5%	2%
Total Revenue⁽²⁾	\$ 2,444	\$ 2,498	(2.2)%	(1.6)%	100%	100%
Memo:						
Xerox Services ⁽³⁾	\$ 870	\$ 917	(5.1)%	(4.5)%	36%	37%

CC - Constant Currency (see "Non-GAAP Financial Measures" section).

⁽¹⁾ Certain prior year amounts have been conformed to the current year presentation. See Appendix III for this change in presentation.

⁽²⁾ Refer to Appendix II for our Geographic Sales Channels and Products and Offerings Definitions.

⁽³⁾ Excluding equipment revenue, Xerox Services was \$751 million and \$786 million in the fourth quarter 2019 and 2018, respectively, representing a decrease of 4.5% including a 0.7-percentage point unfavorable impact from currency.

Fourth quarter 2019 total revenue decreased 2.2% as compared to fourth quarter 2018, including a 0.6-percentage point unfavorable impact from currency, and an approximate 3.1-percentage point favorable impact from a fee of \$77 million received in exchange for an OEM license of certain intellectual property to Fuji Xerox. See the "Sales of Ownership Interests in Fuji Xerox Co., Ltd. and Xerox International Partners" section for further details. Fourth quarter 2019 total revenue reflected the following:

- **Post sale revenue** primarily reflects contracted services, equipment maintenance, supplies and financing. These revenues are associated not only with the population of devices in the field, which is affected by installs and removals, but also by the page volumes generated from the usage of such devices, and the revenue per printed page. Post sale revenue also includes transactional IT hardware sales and implementation services from our XBS organization. Post sale revenue decreased 2.2% as compared to fourth quarter 2018, including a 0.5-percentage point unfavorable impact from currency, and an approximate 4.1-percentage point favorable impact from the OEM license fee described above. The decline in post sale revenue reflected the following:
 - **Services, maintenance and rentals revenue** includes rental and maintenance revenue (including bundled supplies) as well as the post sale component of the document services revenue from our Xerox Services offerings. These revenues decreased 0.7% as compared to fourth quarter 2018, including a 0.5-percentage point unfavorable impact from currency and an approximate 5.2-percentage point favorable impact from the OEM license fee described above. The decline at constant currency¹ reflected the continuing trends of lower page volumes (including a higher mix of lower average-page-volume products), an ongoing competitive price environment, and a lower population of devices, which are partially associated with continued lower Enterprise signings and lower installs in prior and current periods.
 - **Supplies, paper and other sales** includes unbundled supplies and other sales. These revenues decreased 7.9% as compared to fourth quarter 2018, including a 0.6-percentage point unfavorable

impact from currency and reflected the timing impact of prior year transactional IT sales from our XBS organization along with lower paper sales from developing markets (primarily from the Latin America region), as well as the impact of lower supplies revenues primarily associated with lower page volume trends.

- **Financing revenue** is generated from financed equipment sale transactions. The 6.3% decline in these revenues reflected a continued decline in the finance receivables balance due to lower equipment sales in prior periods and included a 0.4-percentage point unfavorable impact from currency.

(in millions)	Three Months Ended December 31,		% Change	CC % Change	% of Equipment Sales	
	2019	2018			2019	2018
Entry	\$ 63	\$ 66	(4.5)%	(4.2)%	10%	11%
Mid-range	408	418	(2.4)%	(2.0)%	66%	66%
High-end	139	137	1.5%	1.9%	23%	22%
Other	6	8	(25.0)%	(25.0)%	1%	1%
Equipment Sales	\$ 616	\$ 629	(2.1)%	(1.5)%	100%	100%

CC - Constant Currency (see "Non-GAAP Financial Measures" section).

- **Equipment sales revenue** decreased 2.1% as compared to fourth quarter 2018, including a 0.6-percentage point unfavorable impact from currency as well as the impact of price declines of approximately 5%. The decline at constant currency¹ was primarily driven by lower sales of our office-centric devices (entry and mid-range products) partially offset by higher sales of our production-centric systems (high-end) as well as the benefit of targeted price actions. The decline at constant currency¹ reflected the following:
 - **Entry** - The decrease was primarily due to lower sales of devices from developing market regions in the Americas, as well as lower sales through our indirect channels in EMEA and the U.S.
 - **Mid-range** - The decrease was driven by lower sales from EMEA, reflecting in part continued weakness and delayed decisions associated with uncertainty in the economic environment, partially offset by higher sales from our Americas region, primarily related to our U.S. Enterprise organization which had higher activity from light-production devices associated with the recent launch of PrimeLink (an entry-level production printer) and the benefit of a large account refresh cycle. The decrease was also impacted by lower sales from our U.S. indirect channels and from our XBS sales organization, which continued to recover from the impact of organizational changes earlier in the year that were part of our Project Own It transformation actions (including the transitioning of accounts to implement coverage changes, consolidation of real estate locations and the reduction of management layers).
 - **High-end** - The increase reflected primarily global demand for our newly-launched Baltoro inkjet press, and higher sales from new business and trade-ins of our Iridesse and iGen laser color systems in the U.S., partially offset by lower sales of Versant, our lower-end production systems. The increase also benefited from higher sales of black-and-white systems in the U.S. as a result of the timing of our customers' renewal cycles.

Total Installs

Installs reflect new placement of devices only (i.e., measure does not take into account removal of devices which may occur as a result of contract renewals or cancellations). Revenue associated with equipment installations may be reflected up-front in Equipment sales or over time either through rental income or as part of our Xerox Services revenues (which are both reported within our post sale revenues), depending on the terms and conditions of our agreements with customers. Installs include activity from Xerox Services and Xerox-branded products shipped to our XBS sales unit. Detail by product group (see Appendix II) is shown below:

Entry

- 2% decrease in color multifunction devices reflecting lower installs of ConnectKey devices primarily from EMEA, partially offset by higher installs from our indirect channels in the U.S.
- 9% decrease in black-and-white multifunction devices reflecting lower activity primarily from our indirect channels in the U.S. and from developing regions in the Americas.

Mid-Range²

- 8% decrease in mid-range color installs primarily reflecting lower installs of multifunction color devices partially offset by higher installs of light-production devices that sit at the higher end of the portfolio range.
- 19% decrease in mid-range black-and-white reflecting in part global market trends.

High-End²

- 12% decrease in high-end color installs reflecting lower installs of our lower-end Versant production systems, partially offset by global demand for our newly-launched Baltoro inkjet press, and higher installs of our Iridesse color systems in the U.S.
- 8% increase in high-end black-and-white systems as a result of higher sales in the U.S. associated with the timing of our customers' renewal cycles which offset declining market trends.

⁽¹⁾ See the "Non-GAAP Financial Measures" section for an explanation of the non-GAAP financial measure.

⁽²⁾ Mid-range and High-end color installations exclude Fuji Xerox digital front-end sales; including Fuji Xerox digital front-end sales, Mid-range color devices decreased 9%, and High-end color systems decreased 11%.

Costs, Expenses and Other Income

Summary of Key Financial Ratios

The following is a summary of key financial ratios used to assess our performance:

(in millions)	Three Months Ended December 31,		
	2019	2018	B/(W)
Gross Profit	\$ 1,016	\$ 998	\$ 18
RD&E	93	94	1
SAG	512	552	40
Equipment Gross Margin	32.0%	33.2%	(1.2) pts.
Post sale Gross Margin	44.8%	42.2%	2.6 pts.
Total Gross Margin	41.6%	40.0%	1.6 pts.
RD&E as a % of Revenue	3.8%	3.8%	— pts.
SAG as a % of Revenue	20.9%	22.1%	1.2 pts.
Pre-tax Income	\$ 336	\$ 124	\$ 212
Pre-tax Income Margin	13.7%	5.0%	8.7 pts.
Adjusted ⁽¹⁾ Operating Profit	\$ 411	\$ 352	\$ 59
Adjusted ⁽¹⁾ Operating Margin	16.8%	14.1%	2.7 pts.

⁽¹⁾ See the "Non-GAAP Financial Measures" section for an explanation of the non-GAAP financial measure.

Pre-tax Income Margin

Fourth quarter 2019 pre-tax income margin of 13.7% increased 8.7-percentage points as compared to fourth quarter 2018. The increase reflected lower Other expenses, net, as well as an approximate 2.8-percentage point favorable impact from the \$77 million OEM license fee described above, and lower operating expenses which offset the adverse impact of lower revenues.

Adjusted¹ Operating Margin

Fourth quarter 2019 adjusted¹ operating margin of 16.8% increased by 2.7-percentage points as compared to fourth quarter 2018 primarily reflecting an approximate 2.7-percentage point favorable impact from the OEM license fee described above. The increase also reflected the impact of cost and expense reductions associated with our Project Own It transformation actions, offset by the impact of lower revenues and an approximate 0.3-percentage point unfavorable impact from transaction currency.

⁽¹⁾ Refer to the Operating Income and Margin reconciliation table in the "Non-GAAP Financial Measures" section.

Gross Margin

Fourth quarter 2019 gross margin of 41.6% increased by 1.6-percentage points compared to fourth quarter 2018, reflecting an approximate 1.9-percentage point favorable impact from the OEM license fee described above, as well as the benefits from our Project Own It transformation actions which offset the impact of lower revenues as well as an approximate 0.3-percentage point unfavorable impact from transaction currency and an approximate 0.4-percentage point unfavorable impact from incremental tariff costs.

Fourth quarter 2019 equipment gross margin of 32.0% decreased by 1.2-percentage points as compared to fourth quarter 2018, reflecting an approximate 1.2-percentage point unfavorable impact from incremental tariff costs. The favorable mix of sales of high-end devices, and cost productivity offset the impact of lower revenues and selective price actions and an approximate 0.7-percentage point unfavorable impact from transaction currency.

Fourth quarter 2019 post sale gross margin of 44.8% increased by 2.6-percentage points as compared to fourth quarter 2018, including an approximate 2.4-percentage point favorable impact from the OEM license fee described above, as well as productivity and restructuring savings associated with our Project Own It transformation actions, which entirely offset the impact of lower revenues, including lower pricing on contract renewals, and an approximate 0.2-percentage point unfavorable impact from transaction currency.

Gross margins are expected to continue to be negatively impacted in future periods as a result of an increase in the cost of our imported products due to higher import tariffs. We are taking actions to mitigate the impact of these tariffs, such as raising prices on certain products, however, we currently estimate an approximately \$35 million cost impact from these higher tariffs in 2020.

Research, Development and Engineering Expenses (RD&E)

Fourth quarter 2019 RD&E as a percentage of revenue of 3.8% was flat as compared to fourth quarter 2018, primarily due to lower expenses offset by the impact of revenues declines.

RD&E of \$93 million decreased \$1 million as compared to fourth quarter 2018.

Selling, Administrative and General Expenses (SAG)

SAG as a percentage of revenue of 20.9% decreased by 1.2-percentage points as compared to fourth quarter 2018, primarily reflecting the benefit from productivity and restructuring associated with our Project Own It transformation actions which offset the impact from lower revenues.

SAG of \$512 million decreased by \$40 million as compared to fourth quarter 2018, reflecting productivity and restructuring savings associated with our Project Own It transformation actions as well as the year-over-year benefit of \$10 million of charges in the prior year related to the cancellation of certain IT projects, offset by higher performance incentive compensation as well as higher advertising investments primarily in indirect channel marketing. Bad debt expense of \$8 million was \$7 million higher compared to fourth quarter 2018 primarily due to an increased level of sales-type leases as a result of our adoption of ASC Topic 842 - Leases and associated changes in the collectibility assessment of certain leases as well as an increased mix of high-end equipment sales. On a trailing twelve-month basis (TTM), bad debt expense remained at less than one percent of total receivables.

Restructuring and Related Costs

During the second half of 2018, we started our Project Own It transformation initiative. The primary goal of this initiative is to improve productivity by driving end-to-end transformation of our processes and systems to create greater focus, speed, accountability and effectiveness and to reduce costs. We incurred restructuring and related costs of \$53 million for the fourth quarter 2019 primarily related to costs to implement initiatives under our business transformation projects including Project Own It. The following is a breakdown of those costs:

(in millions)	Three Months Ended December 31, 2019
Restructuring Severance ⁽¹⁾	\$ 44
Asset Impairments ⁽²⁾	13
Other contractual termination costs ⁽³⁾	1
Net reversals ⁽⁴⁾	(11)
Restructuring and asset impairment costs	47
Retention related severance/bonuses ⁽⁵⁾	8
Contractual severance costs ⁽⁶⁾	2
Consulting and other costs ⁽⁷⁾	(4)
Total	\$ 53

⁽¹⁾ Reflects headcount reductions of approximately 550 employees worldwide.

⁽²⁾ Primarily related to the exit and abandonment of leased and owned facilities. The charge includes the accelerated write-off of \$3 million for leased right-of-use asset balances and \$10 million for owned asset balances upon exit from the facilities net of any potential sublease income and other recoveries.

⁽³⁾ Primarily include additional costs incurred upon the exit from our facilities including decommissioning costs and associated contractual termination costs.

⁽⁴⁾ Reflects net reversals for changes in estimated reserves from prior period initiatives as well as \$4 million in favorable adjustments from the early termination of prior period impaired leases.

⁽⁵⁾ Includes retention related severance and bonuses for employees expected to continue working beyond their minimum notification period before termination.

⁽⁶⁾ Reflects severance and other related costs we are contractually required to pay on employees transferred (approximately 2,200 employees) as part of the shared service arrangement entered into with HCL Technologies.

⁽⁷⁾ Represents professional support services associated with our business transformation initiatives. The credit in the fourth quarter 2019 reflects adjustments of prior period estimated accruals for services.

Fourth quarter 2019 actions impacted several functional areas, with approximately 47% focused on gross margin improvements, approximately 47% focused on SAG reductions, and the remainder focused on RD&E optimization.

The implementation of our Project Own It initiatives as well as other business transformation initiatives is expected to continue to deliver significant cost savings in 2020. While many initiatives are underway and have yet to yield the full transformation benefits expected upon their completion, the changes implemented thus far have improved our cost structure and are beginning to yield longer term benefits. However, expected savings associated with these initiatives may be offset to some extent by business disruption during the implementation phase as well as investments in new processes and systems until the initiatives are fully implemented and stabilized.

Fourth quarter 2018 restructuring and related costs of \$ 67 million included net restructuring and asset impairment charges of \$66 million and \$1 million of additional costs primarily related to professional support services associated with the business transformation initiatives.

Fourth quarter 2018 net restructuring and asset impairment charges of \$66 million included \$72 million of severance costs related to headcount of approximately 850 employees worldwide and \$1 million of lease cancellation costs. These costs were partially offset by \$7 million of net reversals for changes in estimated reserves from prior period initiatives. Fourth quarter 2018 actions impacted several functional areas, with approximately 15% focused on gross margin improvements, approximately 80% focused on SAG reductions, and the remainder focused on RD&E optimization.

The restructuring reserve balance as of December 31, 2019 for all programs was \$70 million, which is expected to be paid over the next twelve months.

Transaction and Related Costs, Net

We incurred \$4 million of Transaction and related costs, net during fourth quarter 2019 primarily related to legal costs associated with our announced proposal to acquire HP (see the "Proposed Transaction with HP" section for further details). These costs are expected to continue in future periods. This compares to \$5 million of costs incurred during fourth quarter 2018, which were primarily associated with the terminated Fuji transaction.

Amortization of Intangible Assets

Fourth quarter 2019 Amortization of intangible assets of \$ 10 million decreased by \$2 million compared to fourth quarter 2018 as a result of the write-off of trade names in prior periods associated with our realignment and consolidation of certain XBS sales units as part of Project Own It transformation actions.

Worldwide Employment

Worldwide employment was approximately 27,000 as of December 31, 2019 and decreased by approximately 5,400 from December 31, 2018. The reduction resulted from net attrition (attrition net of gross hires), of which a large portion is not expected to be backfilled, as well as the impact of organizational changes including employees transferred as part of the shared services arrangement entered into with HCL Technologies earlier this year.

Other Expenses, Net

(in millions)	Three Months Ended December 31,	
	2019	2018
Non-financing interest expense	\$ 24	\$ 29
Non-service retirement-related costs	(3)	67
Interest income	(7)	(3)
Gains on sales of businesses and assets	(1)	—
Contract termination costs - IT services	(4)	43
Currency losses, net	1	3
Loss on sales of accounts receivable	1	1
All other expenses, net	(3)	4
Other expenses, net	\$ 8	\$ 144

Non-financing interest expense

Fourth quarter 2019 non-financing interest expense of \$24 million was \$5 million lower than fourth quarter 2018. When combined with financing interest expense (Cost of financing), total interest expense decreased by \$4 million from fourth quarter 2018 primarily due to a lower debt balance.

Non-service retirement-related costs

Fourth quarter 2019 non-service retirement-related costs were \$70 million lower than fourth quarter 2018, primarily driven by the favorable impact of a 2018 amendment to our U.S. Retiree Health Plan and lower losses from pension settlements in the U.S.

Interest income

Fourth quarter 2019 interest income was \$4 million higher than fourth quarter 2018, primarily reflecting interest on a higher cash balance as a result of cash proceeds received from the Sales of our indirect 25% equity interest in Fuji Xerox (FX) and indirect 51% partnership interest in Xerox International Partners (XIP) completed on November 8, 2019. See the "Sales of Ownership Interests in Fuji Xerox Co., Ltd. and Xerox International Partners" section for further details.

Contract termination costs - IT services

Contract termination costs - IT services was a \$4 million credit in fourth quarter 2019 (\$12 million for the full year 2019) reflecting an adjustment to the \$43 million penalty recorded in fourth quarter 2018, associated with the termination of an IT services arrangement.

Income Taxes

Fourth quarter 2019 effective tax rate was 21.7%. On an adjusted¹ basis, fourth quarter 2019 effective tax rate was 25.0%. These rates were higher than the U.S. federal statutory tax rate of 21% primarily due to state taxes and the geographical mix of profits. The adjusted¹ effective tax rate excludes the tax impacts associated with the following charges: Restructuring and related costs, Amortization of intangible assets, Transaction and related costs, net as well as non-service retirement-related costs and other discrete, unusual or infrequent items as described in our Non-GAAP Financial Measures section.

Fourth quarter 2018 effective tax rate was 27.4% and included a reduction of \$6 million related to a change in the provisional estimated impact from the 2017 Tax Cuts Jobs Act (the "Tax Act"). On an adjusted¹ basis, fourth quarter 2018 effective tax rate was 27.7%. This rate was higher than the U.S. federal statutory tax rate of 21% primarily due to state taxes and the geographical mix of profits. The adjusted¹ effective tax rate excludes the tax impacts associated with the following charges: Restructuring and related costs, Amortization of intangible assets, Transaction and related costs, net, non-service retirement-related costs as well as other discrete, unusual or infrequent items as described in our Non-GAAP Financial Measures section, which include the impact of the Tax Act.

Our effective tax rate is based on nonrecurring events as well as recurring factors, including the taxation of foreign income. In addition, our effective tax rate will change based on discrete or other nonrecurring events that may not be predictable.

⁽¹⁾ Refer to the Effective Tax Rate reconciliation table in the "Non-GAAP Financial Measures" section.

Net Income from Continuing Operations

Fourth quarter 2019 net income from continuing operations attributable to Xerox Holdings was \$266 million, or \$1.17 per diluted share. On an adjusted¹ basis, net income from continuing operations attributable to Xerox Holdings was \$300 million, or \$1.33 per diluted share. Fourth quarter 2019 adjustments to net income from continuing operations included Restructuring and related costs, Amortization of intangible assets, Transaction and related cost, net as well as non-service retirement-related costs and other discrete, unusual or infrequent items as described in our Non-GAAP Financial Measures section.

Fourth quarter 2018 net income from continuing operations attributable to Xerox Holdings was \$91 million, or \$0.37 per diluted share. On an adjusted¹ basis, net income from continuing operations attributable to Xerox Holdings was \$231 million, or \$0.94 per diluted share. Fourth quarter 2018 adjustments to net income from continuing operations

included Restructuring and related costs, Amortization of intangible assets, Transaction and related costs, net as well as non-service retirement-related costs and other discrete, unusual or infrequent items as described in our Non-GAAP Financial Measures section.

(1) Refer to the "Non-GAAP Financial Measures" section for the calculation of adjusted EPS. The calculations of basic and diluted earnings per share are included as Appendix I.

Discontinued Operations

In November 2019, Xerox Holdings completed a series of transactions to restructure its relationship with FUJIFILM Holdings Corporation ("FH"), including the sale of its indirect 25% equity interest in Fuji Xerox ("FX") for approximately \$2.2 billion as well as the sale of its indirect 51% partnership interest in Xerox International Partners ("XIP") for approximately \$23 million (collectively the "Sales").

The Sales resulted in a pre-tax gain of \$629 million (\$539 million after-tax), which was net of approximately \$9 million of transaction costs and \$8 million of allocated goodwill associated with our XIP business. The XIP allocated goodwill was based on the relative fair value of our XIP business, as evidenced by the sales price, as compared to the total estimated fair value of Xerox. No Goodwill was allocated for our investment in FX based on consideration of the guidance in ASC 350-20-40-2 and the fact that an equity investment is not considered a business in accordance with ASC 805-10-55, as it was not controlled by Xerox.

(in millions)	Three Months Ended December 31,	
	2019	2018
Revenue	\$ 6	\$ 35
Income from operations ⁽¹⁾	\$ 14	\$ 52
Gain on disposal	629	—
Income before income taxes	643	52
Income tax expense	(90)	(3)
Income from discontinued operations, net of tax	\$ 553	\$ 49
Income from discontinued operations attributable to noncontrolling interests, net of tax	(1)	(3)
Income from discontinued operations, net of tax attributable to Xerox Holdings	\$ 552	\$ 46

(in millions)	Year Ended December 31,	
	2019	2018
Revenue	\$ 79	\$ 168
Income from operations ⁽¹⁾	\$ 176	\$ 73
Gain on disposal	629	—
Income before income taxes	805	73
Income tax expense	(95)	(9)
Income from discontinued operations, net of tax	\$ 710	\$ 64
Income from discontinued operations attributable to noncontrolling interests, net of tax	(5)	(9)
Income from discontinued operations, net of tax attributable to Xerox Holdings	\$ 705	\$ 55

⁽¹⁾ Includes equity income from FX of \$15 million and \$37 million for the Three Months Ended December 31, 2019 and 2018, respectively, and \$147 million and \$25 million for the Year Ended December 31, 2019 and 2018, respectively.

Capital Resources and Liquidity

The following summarizes our cash, cash equivalents and restricted cash:

(in millions)	Three Months Ended December 31,		
	2019	2018	Change
Net cash provided by operating activities of continuing operations	\$ 398	\$ 384	\$ 14
Net cash provided by operating activities of discontinued operations	40	31	9
Net cash provided by operating activities	438	415	23
Net cash (used in) provided by investing activities of continuing operations	(17)	11	(28)
Net cash provided by investing activities of discontinued operations	2,233	—	2,233
Net cash provided by investing activities	2,216	11	2,205
Net cash used in financing activities of continuing operations	(851)	(485)	(366)
Net cash used in financing activities of discontinued operations	—	(1)	1
Net cash used in financing activities	(851)	(486)	(365)
Effect of exchange rate changes on cash, cash equivalents and restricted cash	13	(10)	23
Increase (decrease) in cash, cash equivalents and restricted cash	1,816	(70)	1,886
Cash, cash equivalents and restricted cash at beginning of period	979	1,218	(239)
Cash, Cash Equivalents and Restricted Cash at End of Period⁽¹⁾	\$ 2,795	\$ 1,148	\$ 1,647

⁽¹⁾ Balance at December 31, 2018 includes \$3 million associated with discontinued operations.

Cash Flows from Operating Activities

Net cash provided by operating activities from continuing operations was \$398 million in fourth quarter 2019. The \$14 million increase in operating cash from fourth quarter 2018 was primarily due to the following:

- \$58 million increase from after-tax impact of the OEM license agreement with FX.
- \$18 million net increase from finance assets reflecting \$26 million increase from lower placements of equipment on operating leases partially offset by \$8 million decrease from higher finance receivables.
- \$20 million increase from accrued compensation primarily related to lower compensation costs and year-over-year timing of payments.
- \$14 million increase from lower restructuring and related payments primarily due to timing of initiatives and associated payments.
- \$48 million decrease as a result of lower fourth quarter inventory reductions in 2019 as compared to the prior year primarily due to timing of purchases.
- \$42 million decrease from accounts receivable primarily due to the timing of collections.

Cash Flows from Investing Activities

Net cash used in investing activities of continuing operations was \$17 million in fourth quarter 2019. The \$28 million change from fourth quarter 2018 was primarily due to proceeds from the sale of buildings in Ireland in the prior year.

Cash Flows from Financing Activities

Net cash used in financing activities of continuing operations was \$851 million in fourth quarter 2019. The \$366 million increase in the use of cash from fourth quarter 2018 was primarily due to the following:

- \$550 million increase from net debt activity primarily due to payments of \$554 million on maturing Senior Notes in fourth quarter 2019 compared to no payments in prior year.
- \$184 million decrease from lower share repurchases due to timing.

Adoption of New Leasing Standard

On January 1, 2019, we adopted ASU 2016-02, Leases (ASC Topic 842). This update, as well as additional amendments and targeted improvements issued in 2018 and early 2019, supersedes existing lease accounting guidance found under ASC 840, Leases (ASC 840) and requires the recognition of right-of-use (ROU) assets and lease obligations by lessees for those leases originally classified as operating leases under prior lease guidance.

Upon adoption, we applied the transition option, whereby prior comparative periods are not retrospectively presented in the Condensed Consolidated Financial Statements. Lessee accounting - the adoption of this update resulted in an increase to assets and related liabilities of approximately \$385 million (approximately \$440 million undiscounted) primarily related to leases of facilities. Lessor accounting - the adoption of this update resulted in an increase to equipment sales of approximately \$10 million in fourth quarter 2019. The adoption of the new standard did not, nor is it expected to, have a material impact on our results of operations or cash flows.

Operating leases ROU assets, net and operating lease liabilities were reported in the Condensed Consolidated Balance Sheets as follows:

(in millions)	December 31, 2019
Other long-term assets	\$ 319
Accrued expenses and other current liabilities	\$ 87
Other long-term liabilities	260
Total Operating lease liabilities	\$ 347

Cash, Cash Equivalents and Restricted Cash

Restricted cash primarily relates to escrow cash deposits made in Brazil associated with ongoing litigation. Various litigation matters in Brazil require us to make cash deposits to escrow as a condition of continuing the litigation. Restricted cash amounts are classified in our Condensed Consolidated Balance Sheets based on when the cash is expected to be contractually or judicially released.

(in millions)	December 31, 2019	December 31, 2018
Cash and cash equivalents	\$ 2,740	\$ 1,081
Restricted cash		
Litigation deposits in Brazil	55	61
Other restricted cash	—	3
Total Restricted cash	55	64
Cash, cash equivalents and restricted cash	2,795	1,145
Cash, cash equivalents and restricted cash - discontinued operations	—	3
Cash, cash equivalents and restricted cash - total	\$ 2,795	\$ 1,148

Restricted cash was reported in the Condensed Consolidated Balance Sheets as follows:

(in millions)	December 31, 2019	December 31, 2018
Other current assets	\$ —	\$ 1
Other long-term assets	55	63
Total Restricted cash	\$ 55	\$ 64

Debt and Customer Financing Activities

The following summarizes our debt:

(in millions)	December 31, 2019	December 31, 2018
Principal debt balance ⁽¹⁾	\$ 4,313	\$ 5,281
Net unamortized discount	(16)	(25)
Debt issuance costs	(17)	(25)
Fair value adjustments ⁽²⁾		
- terminated swaps	1	2
- current swaps	1	(3)
Total Debt	\$ 4,282	\$ 5,230

⁽¹⁾ There were no Notes Payable as of December 31, 2019 and December 31, 2018.

⁽²⁾ Fair value adjustments include the following: (i) fair value adjustments to debt associated with terminated interest rate swaps, which are being amortized to interest expense over the remaining term of the related notes; and (ii) changes in fair value of hedged debt obligations attributable to movements in benchmark interest rates. Hedge accounting requires hedged debt instruments to be reported inclusive of any fair value adjustment.

Finance Assets and Related Debt

The following represents our total finance assets, net associated with our lease and finance operations:

(in millions)	December 31, 2019	December 31, 2018
Total finance receivables, net ⁽¹⁾	\$ 3,351	\$ 3,472
Equipment on operating leases, net	364	442
Total Finance Assets, net⁽²⁾	\$ 3,715	\$ 3,914

⁽¹⁾ Includes (i) Billed portion of finance receivables, net, (ii) Finance receivables, net and (iii) Finance receivables due after one year, net as included in our Condensed Consolidated Balance Sheets.

⁽²⁾ The change from December 31, 2018 includes an increase of \$3 million due to currency.

Our lease contracts permit customers to pay for equipment over time rather than at the date of installation; therefore, we maintain a certain level of debt (that we refer to as financing debt) to support our investment in these lease contracts, which are reflected in total finance assets, net. For this financing aspect of our business, we maintain an assumed 7:1 leverage ratio of debt to equity as compared to our finance assets.

Based on this leverage, the following represents the breakdown of total debt between financing debt and core debt:

(in millions)	December 31, 2019	December 31, 2018
Finance receivables debt ⁽¹⁾	\$ 2,932	\$ 3,038
Equipment on operating leases debt	319	387
Financing debt	3,251	3,425
Core debt	1,031	1,805
Total Debt	\$ 4,282	\$ 5,230

⁽¹⁾ Finance receivables debt is the basis for our calculation of "Cost of financing" expense in the Condensed Consolidated Statements of Income.

Sales of Accounts Receivable

Accounts receivable sales arrangements may be utilized in the normal course of business as part of our cash and liquidity management. Accounts receivable sold are generally short-term trade receivables with payment due dates of less than 60 days.

Accounts receivable sales activities were as follows:

(in millions)	Three Months Ended December 31,	
	2019	2018
Accounts receivable sales ⁽¹⁾	\$ 128	\$ 108
Loss on sales of accounts receivable	1	1
Estimated increase to operating cash flows ⁽²⁾	67	36

⁽¹⁾ Customers may also enter into structured-payable arrangements that require us to sell our receivables from that customer to a third-party financial institution, which then makes payments to us to settle the customer's receivable. In these instances, we ensure the sale of the receivables are bankruptcy remote and the payment made to us is without recourse. The activity associated with these arrangements is not reflected in this disclosure as payments under these arrangements have not been material and these are customer directed arrangements.

⁽²⁾ Represents the difference between current and prior period accounts receivable sales adjusted for the effects of currency.

Corporate Reorganization

On March 6, 2019, the Xerox Board of Directors approved a reorganization (the "Reorganization") of the Company's corporate structure into a holding company structure. The Reorganization was subject to the approval of shareholders, which was obtained at the annual shareholders meeting held May 21, 2019.

On July 31, 2019, the Reorganization was completed, pursuant to which Xerox (the predecessor publicly held parent company) became a direct, wholly-owned subsidiary of Xerox Holdings. The business operations, directors and executive officers of the Company did not change as a result of the Reorganization.

In this Reorganization, shareholders of Xerox became shareholders of Xerox Holdings on a one-for-one basis; maintaining the same number of shares and ownership percentage as held in Xerox immediately prior to the Reorganization. In addition, the individual holder of the shares of Xerox's Series B Preferred Stock exchanged those shares for the same number of shares of Xerox Holdings Series A Preferred Stock. Each share of Xerox Holdings Series A Preferred Stock has the same designations, rights, powers and preferences, and the same qualifications, limitations and restrictions as the shares of Xerox Series B Preferred Stock, with the addition of certain voting rights. In connection with the Reorganization, Xerox Holdings assumed each of the Xerox stock plans, all unexercised and unexpired options to purchase Xerox common stock and each right to acquire or vest in a share of Xerox common stock, including restricted stock unit awards, performance share awards and deferred stock units that are outstanding under the Xerox stock plans. In addition, Xerox Holdings became a guarantor of Xerox's existing Credit Facility.

The Reorganization was accounted for as a transaction among entities under common control and is expected to be a tax-free transaction for U.S. federal income tax purposes. Shares of Xerox Holdings common stock trade on the New York Stock Exchange under the ticker symbol "XRX", formerly used by Xerox.

Shared Services Arrangement with HCL Technologies

In March 2019, as part of Project Own It, Xerox entered into a shared services arrangement with HCL Technologies ("HCL") pursuant to which we are transitioning certain global administrative and support functions, including, among others, selected information technology and finance functions (excluding accounting), from Xerox to HCL. This transition is expected to take up to 18 months. HCL is expected to make certain up-front and ongoing investments in software, tools and other technology to consolidate, optimize and automate the transferred functions with the goal of providing improved service levels and significant cost savings. The shared services arrangement with HCL includes a total aggregate spending commitment by us of approximately \$1.3 billion over the next 7 years (includes approximately \$100 million incurred in 2019). However, we can terminate the arrangement at any time at our discretion, subject to payment of termination fees that decline over the term, or for cause. The spending commitment excludes restructuring and related costs we are expected to incur in connection with the transition of the contemplated functions. See Restructuring and Related Costs within the Costs, Expenses and Other Income section. The transfer of employees associated with the HCL arrangement in certain countries was subject to compliance with works council and other employment regulatory requirements in those countries, which delayed the transfer as well as the expected savings from the arrangement.

During fourth quarter 2019, we incurred net charges of approximately \$35 million associated with this arrangement, which only reflects the cost associated with the employees transferred to date. The cost has been allocated to the various functional expense lines in the Condensed Consolidated Income Statement based on an assessment of the nature and amount of the costs incurred for the various transferred functions prior to their transfer to HCL.

Proposed Transaction with HP

In November 2019, Xerox proposed a business combination transaction with HP Inc. ("HP") in which HP shareholders would receive \$17 per share in cash, and approximately 48% of the pro forma combined company (based on 0.137 Xerox share for each HP share). In January 2020, Xerox obtained \$24 billion in financing commitments to support the proposed business combination transaction with HP. HP has rejected the proposal and refused to engage in mutual due diligence or negotiations regarding the proposal. In January 2020, Xerox nominated a slate of directors to HP's board to be voted on at HP's 2020 annual meeting of stockholders. Xerox intends to continue to pursue the proposed business combination transaction.

Forward-Looking Statements

This release, and other written or oral statements made from time to time by management contain "forward-looking statements" as defined in the Private Securities Litigation Reform Act of 1995. The words "anticipate", "believe", "estimate", "expect", "intend", "will", "should", "targeting", "projecting", "driving" and similar expressions, as they relate to us, our performance and/or our technology, are intended to identify forward-looking statements. These statements reflect management's current beliefs, assumptions and expectations and are subject to a number of factors that may cause actual results to differ materially. Such factors include but are not limited to: our ability to address our business challenges in order to reverse revenue declines, reduce costs and increase productivity so that we can invest in and grow our business; our ability to attract and retain key personnel; changes in economic and political conditions, trade protection measures, licensing requirements and tax laws in the United States and in the foreign countries in which we do business; the imposition of new or incremental trade protection measures such as tariffs and import or export restrictions; changes in foreign currency exchange rates; our ability to successfully develop new products, technologies and service offerings and to protect our intellectual property rights; the risk that multi-year contracts with governmental entities could be terminated prior to the end of the contract term and that civil or criminal penalties and administrative sanctions could be imposed on us if we fail to comply with the terms of such contracts and applicable law; the risk that partners, subcontractors and software vendors will not perform in a timely, quality manner; actions of competitors and our ability to promptly and effectively react to changing technologies and customer expectations; our ability to obtain adequate pricing for our products and services and to maintain and improve cost efficiency of operations, including savings from restructuring actions; the risk that confidential and/or individually identifiable information of ours, our customers, clients and employees could be inadvertently disclosed or disclosed as a result of a breach of our security systems due to cyber attacks or other intentional acts; reliance on third parties, including subcontractors, for manufacturing of products and provision of services; the exit of the United Kingdom from the European Union; our ability to manage changes in the printing environment and expand equipment placements; interest rates, cost of borrowing and access to credit markets; funding requirements associated with our employee pension and retiree health benefit plans; the risk that our operations and products may not comply with applicable worldwide regulatory requirements, particularly environmental regulations and directives and anti-corruption laws; the outcome of litigation and regulatory proceedings to which we may be a party; any impacts resulting from the restructuring of our relationship with Fujifilm Holdings Corporation; the shared services arrangements entered into by us as part of Project Own It; the ultimate outcome of any possible transaction between Xerox Holdings Corporation ("Xerox") and HP Inc. ("HP"), including the possibility that the parties will not agree to pursue a business combination transaction or that the terms of any definitive agreement will be materially different from those proposed; uncertainties as to whether HP will cooperate with Xerox regarding the proposed transaction; the ultimate result should Xerox determine to commence a proxy contest for election of directors to HP's board of directors; Xerox's ability to consummate the proposed transaction with HP; the conditions to the completion of the proposed transaction, including the receipt of any required shareholder approvals and any required regulatory approvals; Xerox's ability to finance the proposed transaction with HP; Xerox's indebtedness, including the substantial indebtedness Xerox expects to incur in connection with the proposed transaction with HP and the need to generate sufficient cash flows to service and repay such debt; the possibility that Xerox may be unable to achieve expected synergies and operating efficiencies within the expected time-frames or at all and to successfully integrate HP's operations with those of Xerox; that such integration may be more difficult, time-consuming or costly than expected; that operating costs, customer loss and business disruption (including, without limitation, difficulties in maintaining relationships with employees, customers or suppliers) may be greater than expected following the proposed transaction or the public announcement of the proposed transaction; the retention of certain key employees may be difficult; and general economic conditions that are less favorable than expected. Additional risks that may affect Xerox's operations and other factors that are set forth in the "Risk Factors" section, the "Legal Proceedings" section, the "Management's Discussion and Analysis of Financial Condition and Results of Operations" section and other sections of Xerox Corporation's 2018 Annual Report on Form 10-K, as well as in Xerox Corporation's and Xerox Holdings Corporation's Quarterly Reports on Form 10-Q and Current Reports on Form 8-K filed with the SEC. These forward-looking statements speak only as of the date of this release or as of the date to which they refer, and Xerox assumes no obligation to update any forward-looking statements as a result of new information or future events or developments, except as required by law.

Non-GAAP Financial Measures

We have reported our financial results in accordance with generally accepted accounting principles (GAAP). In addition, we have discussed our financial results using the non-GAAP measures described below. We believe these non-GAAP measures allow investors to better understand the trends in our business and to better understand and compare our results. Accordingly, we believe it is necessary to adjust several reported amounts, determined in accordance with GAAP, to exclude the effects of certain items as well as their related income tax effects.

A reconciliation of these non-GAAP financial measures to the most directly comparable financial measures calculated and presented in accordance with GAAP are set forth below as well as in the fourth quarter 2019 presentation slides available at www.xerox.com/investor.

These non-GAAP financial measures should be viewed in addition to, and not as a substitute for, the company's reported results prepared in accordance with GAAP.

Adjusted Earnings Measures

- Net Income and Earnings per share (EPS)
- Effective Tax Rate

The above measures were adjusted for the following items:

- Restructuring and related costs: Restructuring and related costs include restructuring and asset impairment charges as well as costs associated with our transformation programs beyond those normally included in restructuring and asset impairment charges. Restructuring consists of costs primarily related to severance and benefits paid to employees pursuant to formal restructuring and workforce reduction plans. Asset impairment includes costs incurred for those assets sold, abandoned or made obsolete as a result of our restructuring actions, exiting from a business or other strategic business changes. Additional costs for our transformation programs are primarily related to the implementation of strategic actions and initiatives and include third-party professional service costs as well as one-time incremental costs. All of these costs can vary significantly in terms of amount and frequency based on the nature of the actions as well as the changing needs of the business. Accordingly, due to that significant variability, we will exclude these charges since we do not believe they provide meaningful insight into our current or past operating performance nor do we believe they are reflective of our expected future operating expenses as such charges are expected to yield future benefits and savings with respect to our operational performance.
- Amortization of intangible assets: The amortization of intangible assets is driven by our acquisition activity which can vary in size, nature and timing as compared to other companies within our industry and from period to period. The use of intangible assets contributed to our revenues earned during the periods presented and will contribute to our future period revenues as well. Amortization of intangible assets will recur in future periods.
- Transaction and related costs, net: Transaction and related costs, net are expenses incurred in connection with i) our announced proposal to acquire HP Inc. and ii) our planned transaction with Fuji, which was terminated in May 2018, inclusive of costs related to litigation resulting from the terminated transaction and other shareholder actions. The costs are primarily for third-party legal, accounting, consulting and other similar type professional services as well as potential legal settlements. These costs are considered incremental to our normal operating charges and were incurred or are expected to be incurred solely as a result of the planned transactions. Accordingly, we are excluding these expenses from our Adjusted Earnings Measures in order to evaluate our performance on a comparable basis.
- Non-service retirement-related costs: Our defined benefit pension and retiree health costs include several elements impacted by changes in plan assets and obligations that are primarily driven by changes in the debt and equity markets as well as those that are predominantly legacy in nature and related to employees who are no longer providing current service to the company (e.g. retirees and ex-employees). These elements include (i) interest cost, (ii) expected return on plan assets, (iii) amortization of prior plan amendments, (iv) amortized actuarial gains/losses and (v) the impacts of any plan settlements/curtailments. Accordingly, we consider these elements of our periodic retirement plan costs to be outside the operational performance of the business or legacy costs and not necessarily indicative of current or future cash flow requirements. This approach is consistent with the classification of these costs as non-operating in other expenses, net. Adjusted earnings will continue to include the service cost elements of our retirement costs, which is related to current employee service as well as the cost of our defined contribution plans.

- Other discrete, unusual or infrequent items: We excluded the following items given their discrete, unusual or infrequent nature and their impact on our results for the period.
 - Contract termination costs - IT services.
 - Impacts associated with the Tax Cuts and Jobs Act (the "Tax Act") enacted in December 2017.

We believe the exclusion of these items allows investors to better understand and analyze the results for the period as compared to prior periods and expected future trends in our business.

Adjusted Operating Income/Margin

We calculate and utilize adjusted operating income and margin measures by adjusting our reported pre-tax income and margin amounts. In addition to the costs and expenses noted as adjustments for our Adjusted Earnings measures, adjusted operating income and margin also exclude the remaining amounts included in Other expenses, net, which are primarily non-financing interest expense and certain other non-operating costs and expenses. We exclude these amounts in order to evaluate our current and past operating performance and to better understand the expected future trends in our business.

Constant Currency

To better understand trends in our business, we believe that it is helpful to adjust revenue to exclude the impact of changes in the translation of foreign currencies into U.S. dollars. We refer to this adjusted revenue as "constant currency." This impact is calculated by translating current period activity in local currency using the comparable prior year period's currency translation rate. This impact is calculated for all countries where the functional currency is not the U.S. dollar. Management believes the constant currency measure provides investors an additional perspective on revenue trends. Currency impact can be determined as the difference between actual growth rates and constant currency growth rates.

Free Cash Flow

To better understand trends in our business, we believe that it is helpful to adjust operating cash flows by subtracting amounts related to capital expenditures. Management believes this measure gives investors an additional perspective on cash flow from operating activities in excess of amounts required for reinvestment. It provides a measure of our ability to fund acquisitions, dividends and share repurchase.

Summary:

Management believes that all of these non-GAAP financial measures provide an additional means of analyzing the current period's results against the corresponding prior period's results. However, these non-GAAP financial measures should be viewed in addition to, and not as a substitute for, the company's reported results prepared in accordance with GAAP. Our non-GAAP financial measures are not meant to be considered in isolation or as a substitute for comparable GAAP measures and should be read only in conjunction with our consolidated financial statements prepared in accordance with GAAP. Our management regularly uses our supplemental non-GAAP financial measures internally to understand, manage and evaluate our business and make operating decisions. These non-GAAP measures are among the primary factors management uses in planning for and forecasting future periods. Compensation of our executives is based in part on the performance of our business based on these non-GAAP measures.

A reconciliation of these non-GAAP financial measures and the most directly comparable measures calculated and presented in accordance with GAAP are set forth on the following tables:

Net Income and EPS reconciliation

(in millions, except per share amounts)	Three Months Ended December 31,				Year Ended December 31,			
	2019		2018		2019		2018	
	Net Income	EPS	Net Income	EPS	Net Income	EPS	Net Income	EPS
Reported⁽¹⁾	\$ 266	\$ 1.17	\$ 91	\$ 0.37	\$ 648	\$ 2.78	\$ 306	\$ 1.16
Adjustments:								
Restructuring and related costs	53		67		229		157	
Amortization of intangible assets	10		12		45		48	
Transaction and related costs, net	4		5		12		68	
Non-service retirement-related costs	(3)		67		18		150	
Contract termination costs - IT services	(4)		43		(12)		43	
Income tax on adjustments ⁽²⁾	(22)		(48)		(77)		(116)	
Tax Act	(4)		(6)		(35)		89	
Adjusted	\$ 300	\$ 1.33	\$ 231	\$ 0.94	\$ 828	\$ 3.55	\$ 745	\$ 2.88
Dividends on preferred stock used in adjusted EPS calculation ⁽³⁾		—		—		—		—
Weighted average shares for adjusted EPS ⁽³⁾		227		246		233		258
Fully diluted shares at end of period ⁽⁴⁾		224						

⁽¹⁾ Net income and EPS from continuing operations attributable to Xerox Holdings.

⁽²⁾ Refer to Effective Tax Rate reconciliation.

⁽³⁾ For those periods that exclude the preferred stock dividend, the average shares for the calculations of diluted EPS include 7 million shares associated with our Series A convertible preferred stock, as applicable.

⁽⁴⁾ Represents common shares outstanding at December 31, 2019 as well as shares associated with our Series A convertible preferred stock plus potential dilutive common shares as used for the calculation of diluted earnings per share for the fourth quarter 2019.

Effective Tax Rate reconciliation

(in millions)	Three Months Ended December 31, 2019			Three Months Ended December 31, 2018		
	Pre-Tax Income	Income Tax Expense	Effective Tax Rate	Pre-Tax Income	Income Tax Expense	Effective Tax Rate
	Reported⁽¹⁾	\$ 336	\$ 73	21.7%	\$ 124	\$ 34
Non-GAAP Adjustments ⁽²⁾	60	22		194	48	
Tax Act	—	4		—	6	
Adjusted⁽³⁾	\$ 396	\$ 99	25.0%	\$ 318	\$ 88	27.7%

(in millions)	Year Ended December 31, 2019			Year Ended December 31, 2018		
	Pre-Tax Income	Income Tax Expense	Effective Tax Rate	Pre-Tax Income	Income Tax Expense	Effective Tax Rate
	Reported⁽¹⁾	\$ 822	\$ 179	21.8%	\$ 549	\$ 247
Non-GAAP Adjustments ⁽²⁾	292	77		466	116	
Tax Act	—	35		—	(89)	
Adjusted⁽³⁾	\$ 1,114	\$ 291	26.1%	\$ 1,015	\$ 274	27.0%

⁽¹⁾ Pre-tax income and income tax expense from continuing operations.

⁽²⁾ Refer to Net Income and EPS reconciliation for details.

⁽³⁾ The tax impact on Adjusted Pre-Tax Income from continuing operations is calculated under the same accounting principles applied to the Reported Pre-Tax Income under ASC 740, which employs an annual effective tax rate method to the results.

Operating Income / Margin reconciliation

(in millions)	Three Months Ended December 31, 2019			Three Months Ended December 31, 2018		
	Profit	Revenue	Margin	Profit	Revenue	Margin
Reported⁽¹⁾	\$ 336	\$ 2,444	13.7%	\$ 124	\$ 2,498	5.0%
Adjustments:						
Restructuring and related costs	53			67		
Amortization of intangible assets	10			12		
Transaction and related costs, net	4			5		
Other expenses, net	8			144		
Adjusted	<u>\$ 411</u>	<u>\$ 2,444</u>	16.8%	<u>\$ 352</u>	<u>\$ 2,498</u>	14.1%

(in millions)	Year Ended December 31, 2019			Year Ended December 31, 2018		
	Profit	Revenue	Margin	Profit	Revenue	Margin
Reported⁽¹⁾	\$ 822	\$ 9,066	9.1%	\$ 549	\$ 9,662	5.7%
Adjustments:						
Restructuring and related costs	229			157		
Amortization of intangible assets	45			48		
Transaction and related costs, net	12			68		
Other expenses, net	84			271		
Adjusted	<u>\$ 1,192</u>	<u>\$ 9,066</u>	13.1%	<u>\$ 1,093</u>	<u>\$ 9,662</u>	11.3%

⁽¹⁾ Pre-Tax Income and revenue from continuing operations.

Free Cash Flow reconciliation

(in millions)	Three Months Ended December 31,		Year Ended December 31,	
	2019	2018	2019	2018
Reported⁽¹⁾	\$ 398	\$ 384	\$ 1,244	\$ 1,082
Capital Expenditures	(17)	(17)	(65)	(90)
Free Cash Flow	<u>\$ 381</u>	<u>\$ 367</u>	<u>\$ 1,179</u>	<u>\$ 992</u>

⁽¹⁾ Net cash provided by operating activities from continuing operations.

Guidance

Earnings per Share

(in millions, except per share amounts)	FY 2020	
	Net Income	EPS
Estimated⁽¹⁾	\$ 625	~ \$2.80 - \$2.90
Adjustments:		
Restructuring and related costs		175
Amortization of intangible assets		35
Non-service retirement-related costs		35
Income tax on adjustments		(70)
Adjusted	<u>\$ 800</u>	<u>~ \$3.60 - \$3.70</u>
Estimated Full Year 2020 weighted average shares for GAAP and adjusted EPS	220	

⁽¹⁾ Net Income and EPS from continuing operations attributable to Xerox Holdings.

Operating Income / Margin

(in millions)	FY 2020		
	Profit	Revenue ⁽²⁾	Margin
Estimated⁽¹⁾	\$ 845	\$ 8,625	~ 10%
Adjustments:			
Restructuring and related costs	175		
Amortization of intangible assets	35		
Non-service retirement-related costs	35		
Other expenses, net	40		
Adjusted	\$ 1,130	\$ 8,625	~ 13%

⁽¹⁾ Pre-Tax Income and revenue from continuing operations.

⁽²⁾ Full year 2020 revenue reflects an estimated revenue decline at actual currency of approximately 4.9% from FY 2019, or a decline of approximately 4% excluding the impact of the upfront OEM license fee of \$77M in 2019. Impact from translation currency is de minimis.

Free Cash Flow

(in millions)	FY 2020
Operating Cash Flow⁽¹⁾	~ \$1,300
Less: capital expenditures	(100)
Free Cash Flow	~ \$1,200

⁽¹⁾ Net cash provided by operating activities from continuing operations.

APPENDIX I

Xerox Holdings Corporation Earnings per Common Share

(in millions, except per-share data, shares in thousands)	Three Months Ended December 31,		Year Ended December 31,	
	2019	2018	2019	2018
Basic Earnings per Share:				
Net Income from continuing operations attributable to Xerox Holdings	\$ 266	\$ 91	\$ 648	\$ 306
Accrued dividends on preferred stock	(3)	(3)	(14)	(14)
Adjusted net income from continuing operations available to common shareholders	\$ 263	\$ 88	\$ 634	\$ 292
Net income from discontinued operations attributable to Xerox Holdings, net of tax	552	46	705	55
Adjusted net income available to common shareholders	\$ 815	\$ 134	\$ 1,339	\$ 347
Weighted average common shares outstanding	215,499	236,190	221,969	248,707
Basic Earnings per Share:				
Continuing operations	\$ 1.22	\$ 0.37	\$ 2.86	\$ 1.17
Discontinued operations	2.56	0.19	3.17	0.23
Basic Earnings per Share	\$ 3.78	\$ 0.56	\$ 6.03	\$ 1.40
Diluted Earnings per Share:				
Net Income from continuing operations attributable to Xerox Holdings	\$ 266	\$ 91	\$ 648	\$ 306
Accrued dividends on preferred stock	—	(3)	—	(14)
Adjusted net income from continuing operations available to common shareholders	\$ 266	\$ 88	\$ 648	\$ 292
Net income from discontinued operations attributable to Xerox Holdings, net of tax	552	46	705	55
Adjusted net income available to common shareholders	\$ 818	\$ 134	\$ 1,353	\$ 347
Weighted average common shares outstanding	215,499	236,190	221,969	248,707
Common shares issuable with respect to:				
Stock Options	111	—	55	—
Restricted stock and performance shares	4,326	3,188	4,403	2,953
Convertible preferred stock	6,742	—	6,742	—
Adjusted weighted average common shares outstanding	226,678	239,378	233,169	251,660
Diluted Earnings per Share:				
Continuing operations	\$ 1.17	\$ 0.37	\$ 2.78	\$ 1.16
Discontinued operations	2.44	0.19	3.02	0.22
Diluted Earnings per Share	\$ 3.61	\$ 0.56	\$ 5.80	\$ 1.38
The following securities were not included in the computation of diluted earnings per share as they were either contingently issuable shares or shares that if included would have been anti-dilutive:				
Stock options	750	1,022	805	1,022
Restricted stock and performance shares	1,350	2,833	1,272	3,068
Convertible preferred stock	—	6,742	—	6,742
Total Anti-Dilutive Securities	2,100	10,597	2,077	10,832
Dividends per Common Share				
	\$ 0.25	\$ 0.25	\$ 1.00	\$ 1.00

APPENDIX II

Xerox Holdings Corporation Geographic Sales Channels and Product/Offering Definitions

Our business is aligned to a geographic focus and is primarily organized on the basis of go-to-market sales channels, which are structured to serve a range of customers for our products and services. In 2019 we changed our geographic structure to create a more streamlined, flatter and more effective organization, as follows:

- Americas, which includes our sales channels in the U.S. and Canada, as well as Mexico, and Central and South America.
- EMEA, which includes our sales channels in Europe, the Middle East, Africa and India.
- Other, primarily includes sales to and royalties from Fuji Xerox, and our licensing revenue.

Our products and offerings include:

- "Entry", which includes A4 devices and desktop printers. Prices in this product group can range from approximately \$150 to \$3,000.
- "Mid-Range", which includes A3 Office and Light Production devices that generally serve workgroup environments in mid to large enterprises. Prices in this product group can range from approximately \$2,000 to \$75,000+.
- "High-End", which includes production printing and publishing systems that generally serve the graphic communications marketplace and large enterprises. Prices for these systems can range from approximately \$30,000 to \$1,000,000+.
- Xerox Services, formerly known as Managed Document Services (MDS), which includes solutions and services that span from managing print to automating processes to managing content. Our primary offerings are Intelligent Workplace Services (IWS), which is our rebranded Managed Print Services, as well as Digital and Cloud Print Services (including centralized print services). Xerox Services also includes Communication and Marketing Solutions that were previously excluded from our former MDS definition.

APPENDIX III

Change in Presentation

During first quarter 2019, we realigned portions of our business to support our new revenue strategy. This realignment included the combination and consolidation of certain sales units to better service customers consistently across the company. In connection with that realignment, we changed the classification of revenues and those related costs from certain service arrangements to consistently conform the presentation of those amounts among our various business units. Prior year amounts were also revised as follows to conform with the 2019 presentation. The revised presentation does not impact total revenues, total expenses or net income.

	Three Months Ended December 31, 2018		
	As Reported ⁽¹⁾	Change	As Revised
Sales	\$ 1,044	\$ (86)	\$ 958
Services, maintenance and rentals	1,390	86	1,476
Cost of sales	\$ 639	\$ (26)	\$ 613
Cost of services, maintenance and rentals	829	26	855

⁽¹⁾ Sales and Cost of sales from continuing operations.

Describe your plan for quality management and process for continuous improvement of the program for the specified Goods and Services.

Our strategy for University of California will come full circle through our robust customer-oriented tools that drive satisfaction levels and continuous service improvement. Because we understand how crucial prompt and effective service is to your success, Xerox will utilize our Sentinel™ Customer Satisfaction Assurance System to proactively identify and solve any issues at their source. This global, just-in-time tool will allow Xerox to keep a strong pulse on the satisfaction of your end users through a web-based connection between your employees who use our products and services and the Xerox problem solvers dedicated to your account. Sentinel's survey tool communicates with your entire company through e-mail to gather ongoing data and record uncensored feedback from your end users, then automatically creates an electronic problem ticket so that Xerox can make adjustments in real time instead of following up on escalated complaints reactively.

Xerox will use the results of our Sentinel™ program to drive continuous service improvement across University of California's print enterprise. The tool can be used quarterly, annually or on an ad hoc basis—and the results will be brought to life in our in our Quarterly Business Review (QBR) process, through which we will utilize Sentinel™ survey data to gauge your appetite for improvements and further innovation. This ongoing review process will not only strengthen the relationship between University of California end users and Xerox, but also allow us to equip University of California with the printer support tools and services you need to attract and retain the Next Generation of your global workforce.

Additionally, Xerox senior leadership team has committed the entire company to implementing a formal quality assurance program called Xerox Lean Six Sigma (LSS). This strategy provides a fundamental approach to our business and yours. It is a disciplined, data-driven method of reducing waste and variation in processes so they consistently deliver products and services at the quality levels, speeds and prices that our clients value. Our Xerox LSS deployment includes leadership training of senior executives and managers, as well as the specialized training of Master Black Belts, Black Belts and Green Belts. This training ensures the pervasive use of LSS, its tools, and its processes throughout our organization. LSS gives Xerox's management teams a common culture, language, and tool set. Using LSS delivers immediate and continuous improvement results using fact-based decision-making and well-defined metrics. LSS promotes collaboration across traditional functional and work process boundaries inside the company and with our customers. In addition to supporting quality management systems, Xerox solutions also incorporate components that allow our customers to meet many common legal and regulatory requirements. Xerox will work with UC to gain an understanding of specific quality, legal and regulatory requirements to ensure these requirements are met.

As part of our continuing engagement process, UC representatives and the Xerox account team will hold account review meetings on a regular basis, or as requested, focusing on quality management and reviewing the process for continuous improvement. The main objective of these account reviews is to discuss operational and technical issues and performance against standards. Topics discussed may include open issues and progress toward resolution, proposed /impending changes, status of special projects, optimization/future state review, any UC support requirements, UC management support and UC communication needs. Xerox bases its technical service delivery system on using data to evaluate performance. From this method, we can create and build a mutually beneficial business relationship. Our approach will be to report baseline service metrics on a monthly or quarterly basis, as required. Our standard reports will include data on current-month performance as well as trends that accurately show

our extended performance. Our ability to capture and display data in this format allows us to quickly identify and capitalize on any existing performance improvement opportunities.

Please describe in detail your company's delivery and installation capabilities, including fulfillment process from UC purchase order submission to delivery.

Xerox personnel will work with UC to develop a mutually-agreeable implementation plan for delivery, installation, and training. Implementation planning involves three key steps: (1) Pre-Installation, (2) Installation, and (3) Post-Installation. Xerox understands it is responsible for the installation of all equipment and necessary training. As part of the installation process, we conduct standard diagnostic testing, including validating that equipment is producing acceptable copies and printed documents, and that the scanning capabilities are functional. Xerox is not responsible for the cabling of networked devices. When our local delivery carrier receives the equipment order from Xerox, they contact UC to schedule an acceptable delivery date. Upon delivery, the delivery carrier unpacks the system and, based on the products ordered, either a Xerox Customer Service Engineer (CSE) or the delivery carrier handles the installation.

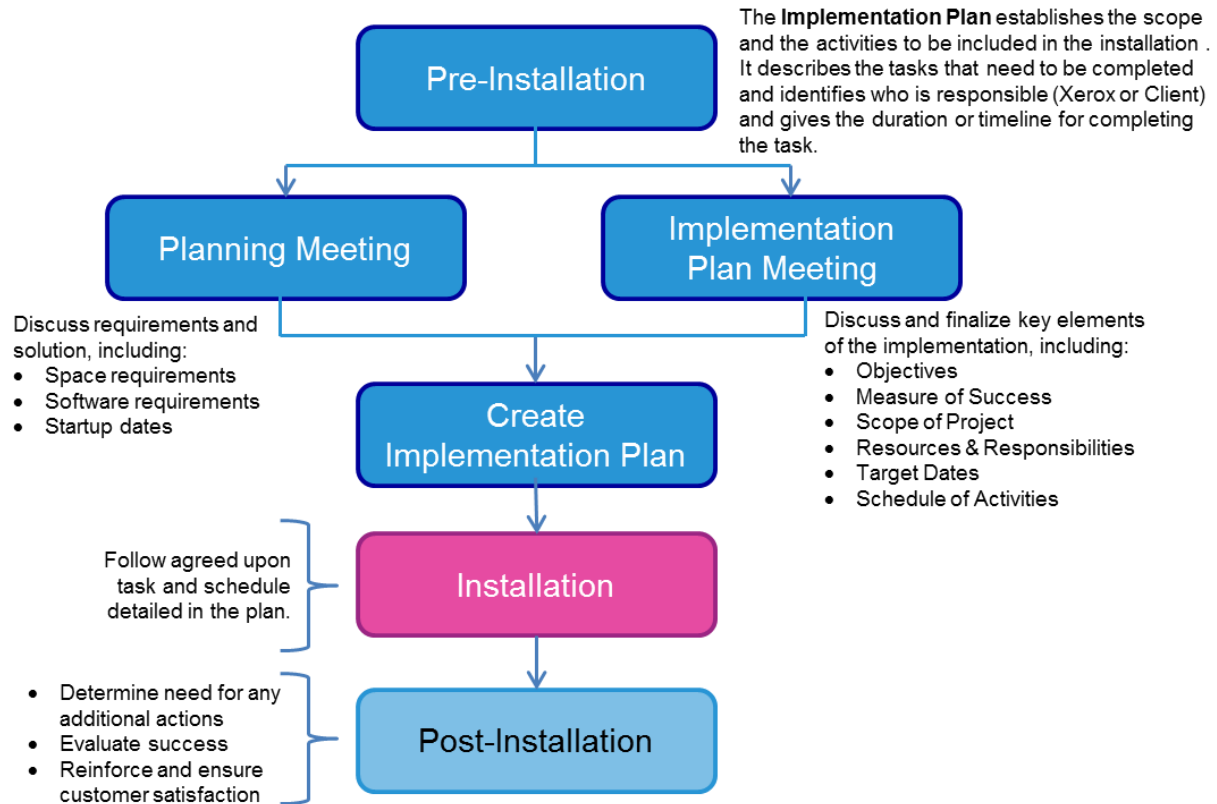
Carrier Installation: After the delivery carrier delivers and unpacks the system, the Analyst "meets the truck" and installs the system hardware. The Analyst also connects all system components prior to powering up the system. Implementation and installation activities are completed to fully enable all features and functions purchased. Then, Xerox provides an overview of basic functionality, including a review of the equipment's software applications. Within 24 hours of installation, your local POC/Sales Executives follows up to ensure customer satisfaction and answer any outstanding questions.

Certain activities require support from UC to ensure a smooth transition and implementation. They include:

- Provide Xerox with sufficient, timely, free and safe access to UC premises for Xerox to fulfil its obligations.
- Name an IT contact as a resource that will ensure all necessary network security, authorization, and authentication credentials are in place. The IT contact should be readily available and able to participate in installation activities.
- Identify network topology and domains and provide a document that maps these to geographical locations served.
- Identify network domains and trust relationships between the domains.
- Identify operating system, including versions and revision levels, associated with the primary domain server.
- Identify what print server operating systems (versions and revision levels) are in use in locations to be serviced.
- Identify network mechanisms for device identification and management on each domain to be serviced, including network address or host name resolution (DNS, Net Bios, etc.).
- Notify Xerox of network, SMTP gateway and Internet proxy server problems.
- Provide (or contract for provision of) all necessary wiring and active network connections.
- Supply IP addresses/subnet masks.

Implementation

Xerox personnel will work with UC to develop a mutually-agreeable implementation plan for delivery, installation, and training. As shown in the following diagram, implementation planning involves three key steps: (1) Pre-Installation, (2) Installation, and (3) Post-Installation.



Xerox understands it is responsible for the installation of all equipment and necessary training. As part of the installation process, we conduct standard diagnostic testing, including validating that equipment is producing acceptable copies and printed documents, and that the scanning capabilities are functional. Xerox is not responsible for the cabling of networked devices.

When our local delivery carrier receives the equipment order from Xerox, they contact UC to schedule an acceptable delivery date. Upon delivery, the delivery carrier unpacks the system and, based on the products ordered, either a Xerox Customer Service Engineer (CSE) or the delivery carrier handles the installation.

CSE Installation (WorkCentre Models): After the delivery carrier delivers and unpacks the system, the CSE “meets the truck” and installs the system hardware. The CSE also connects all system components prior to powering up the system. This is followed up with Analyst Services, at which time all implementation and installation activities are completed to fully enable all features and functions purchased. Then, Xerox provides an overview of basic functionality, including a review of the equipment’s software applications. Within 24 hours of installation, your local POC/Sales Executives follows up to ensure customer satisfaction and answer any outstanding questions.

UC Participation

Certain activities require support from UC to ensure a smooth transition and implementation. They include:

- Provide Xerox with sufficient, timely, free and safe access to UC premises for Xerox to fulfil its obligations.
- Name an IT contact as a resource that will ensure all necessary network security, authorization, and authentication credentials are in place. The IT contact should be readily available and able to participate in installation activities.
- Identify network topology and domains and provide a document that maps these to geographical locations served.
- Identify network domains and trust relationships between the domains.
- Identify operating system, including versions and revision levels, associated with the primary domain server.
- Identify what print server operating systems (versions and revision levels) are in use in locations to be serviced.
- Identify network mechanisms for device identification and management on each domain to be serviced, including network address or host name resolution (DNS, Net Bios, etc.).
- Notify Xerox of network, SMTP gateway and Internet proxy server problems.
- Provide (or contract for provision of) all necessary wiring and active network connections.
- Supply IP addresses/subnet masks.

Change Management

As new floor maps and processes are put into effect, an effective change management plan is designed to ensure a smooth implementation process. We work with UC to create a joint change management plan that minimizes end-user dissatisfaction and accelerates adoption rates. The change management plan includes the following:

- **Communications** - Communication strategy tailored to UC's unique environment
- **Training** - Training strategy and tools tailored to meet user needs
- **Configuration** - Understanding user needs and configuring environment appropriately
- **Transition ("go-live") Support** - Support to assure the best possible transition and implementation

To help understand all the activities that must occur for delivery, installation, and training, we have included a sample Implementation Plan template below. This sample Implementation Plan identifies the implementation task, owner responsible for the completion of the task, and target completion date for each task within the plan.

Implementation Project Plan

Project Tasks Owner(s)	Owner(s)	Target Date
Project Start-Up (After Contract Award)		
Contract Award	UC	TBD
Finalize the implementation requirements Conduct beta testing – gain compliance approvals	UC and Xerox	TBD
Develop communications plan for customer and Xerox employees	UC and Xerox	TBD
Communicate Xerox Project Team responsibilities	Xerox	TBD
Define and communicate Xerox services to team	Xerox	TBD
Locations		
Confirm individual locations	UC and Xerox	TBD
Identify Principals and Key Contacts	UC	TBD
Identify key users	UC and Xerox	TBD
Identify MFD requirements and configurations	Xerox	TBD
Introduce Local Project Team Members	Xerox	TBD
Define and document unique requirements	UC	TBD
Project Start Up Phase Complete		
Installation		
Plan and Design	Xerox	TBD
Validate fleet equipment recommendations and location	UC and Xerox	TBD
Allocate space for equipment removal (if required)	UC	TBD
Confirm delivery requirements	Xerox	TBD
Provide access to loading dock required for Installation Team	UC	TBD
Validate network drop and power requirements	Xerox	TBD
Provide a communication plan during implementation of 'who to call'	Xerox	TBD
Check electric, power, install network drops, fax lines as required	Xerox	TBD
Conduct final Inspection and check to ensure compliance	Xerox	TBD
Order Xerox equipment and software	Xerox	TBD
Deliver Xerox equipment and software	Xerox	TBD
Deploy Xerox equipment and software	Xerox	TBD
Deliver Customer Welcome Kit (if applicable)	Xerox	TBD
Remove existing equipment (if traded)	Xerox	TBD
Install Xerox equipment (delivery carrier or CSE)	Xerox	TBD
Connect Xerox equipment to LAN	UC and Xerox	TBD
Test equipment and confirm install	UC and Xerox	TBD
Test network devices	UC and Xerox	TBD

Project Tasks Owner(s)	Owner(s)	Target Date
Create Print Queues on customer's server	UC and Xerox	TBD
Install Xerox Print Drivers on customer's PCs	UC and Xerox	TBD
Change Print Default to closest Xerox device	UC and Xerox	TBD
Training		
Identify and clarify training requirements for each Location	UC	TBD
Schedule and arrange training – by location	Xerox	TBD
Communicate training schedule to customer staff	UC	TBD
Engage training staff, coordinate training	Xerox	TBD
Provide end-user product CD-ROM	Xerox	TBD
Schedule on-site, "walk-up" training to work groups	Xerox	TBD
Schedule print driver training	Xerox	TBD
Identify additional special training requirements	UC	TBD
Provide links to Brainshark on-demand training	Xerox	TBD
Supplies		
Place Initial Xerox supply order	Xerox	TBD
Order back-up Smart Kits for new devices	Xerox	TBD
Provide supplies reorder list to customer employees	Xerox	TBD
Return old equipment supplies (if required) obtain vendor credit	UC	TBD
Xerox supplies received and validated	Xerox	TBD
Business Processes		
Finalize and communicate billing and reporting process	Xerox	TBD
Develop Invoice Template	Xerox	TBD
Account Management Strategy Developed	Xerox	TBD
Schedule follow-up installation meeting	Xerox	TBD
Develop account review schedule	Xerox	TBD
Develop, test, and train Reporting Processes	UC and Xerox	TBD

Describe the account management team, and all roles thereunder, that you would assign to the UC system if awarded under this RFP, including senior account manager responsible for the entire agreement and UC relationship and local account representatives responsible for each specific UC location. For every role/representative, provide: a description of the role's responsibilities, the name of who will fill this role, their title, and a summary of their qualifications including years of pertinent experience and ALL certifications. Include attachment if necessary.

Xerox is well staffed to support UC's requirement for frequent on-site visitation to support each of your locations. We have a team of 8 regionally based Client Managers, a statewide sales channel model, a team of product and solutions specialist and Higher Ed management leadership who provide localized support to the UC System and the 10 campuses. All of our sales resources are based in California and located within close proximity to the UC campuses they support. This team is supported by two additional California-based Vice President resources that provide contract management, escalation support and strategic value to the team and the UC System.

Xerox offers clients a broad base of skills and professional consulting expertise. Below is a cross section of the background and skills of Xerox project specialists. For those individuals not already part of the account team, we assign specific resources to the University project following contract signature, depending on personnel availability and project requirements.

Account Management

Due to the size and importance of the University of California System, we have aligned two Vice Presidents to support you to provide oversight and involvement in both Northern and Southern California.

Doug MacPhee, Vice President of Sales (16 years with Xerox): Doug's 14 years of experience have focused on all areas of sales and operations management. Covering public sector and higher education, the responsibilities have included managing effective and quality sales objectives as well as the day-to-day operational aspects of some of the largest state and local clients in the the State of California. The Vice President is the University System single point of contact responsible for all aspects of your account, throughout the life of the contract. The VP is accountable for leading initiatives where Xerox can assist you in improving your current situation to increase value to your students, staff, and faculty. The VP is responsible for negotiating and administering client contracts, managing the customer relationships at the System level through delivery and ongoing support, and maintaining a long-term relationship with not only the Office of the President but UC campuses and locations throughout California.

Michelle Yoshino, Regional Vice President (31 years with Xerox): Michelle Yoshino provides this same oversight for all locations in California and is a Co-VP with Doug MacPhee to ensure all aspects of the UC Office of the President and the entire system are managed effectively to ensure the highest levels of customer satisfaction. Her experience includes oversight and management of the largest public sector accounts in the Southwest which include some of our largest Xerox customers.

Jim Potts, Industry Sales Manager (31 years with Xerox): Jim has held a variety of leadership positions in Sales, Sales Management and Marketing Management and is responsible for Sales teams in Northern and Southern California handling major government and higher education customers. Jim prides himself in customer satisfaction and is dedicated to supporting the UC System which encompasses the 10 campuses across the State of California.

Xerox Dedicated UC front line Sales Support Resources in California:

CONSOLIDATED ACCOUNT	REP NAME	REP LOCATION
University of California, Berkeley Lawrence Berkeley National Lab UC Hastings College of Law	Scott Reiber	Bay Area
University of California, Davis University of California, Davis Medical Center	Bill Bennett	Sacramento Area
University of California, Irvine University of California, Irvine Medical Center	Daria Lewis	Orange County Area
University of California, Los Angeles University of California, Los Angeles Medical Center	Martin Soto	Los Angeles Area
University of California, Merced	Bill Bennett	Merced Area
University of California, Office of President	Scott Reiber	Bay Area
University of California, Riverside	Marcia Quo Schmidt	Orange County Area
University of California, San Diego University of California, San Diego Medical Center	Daria Lewis	San Diego Area
University of California, San Francisco University of California, San Francisco Medical Center	Scott Reiber	Bay Area
University of California, Santa Barbara	Marcia Quo Schmidt	Los Angeles Area
University of California, Santa Cruz	Scott Reiber	Bay Area

Scott Reiber, Senior Client Manager (31 years with Xerox): Scott Reiber has been the Account Manager and primary sales and solution executive with 30 years of tenure with Xerox Corporation. His entire Xerox career has been focused on servicing UCSF and Berkeley campus and other higher education institutions in the Bay area. Scott also has the responsibility of supporting the UC Office of the President. He has primary accountability to engage sales specialist team members who can include centralized print, manage print, and other offerings. He provides support and related data for industry trends, security related to our products and day to day support of UCSF initiatives with print. His primary role is to identify, articulate and implement product solutions and services to best suit customer requirements for UCSF.

Scott Reiber, Senior Client Manager (31 years with Xerox): Client Manager for UC Office of the President and UC Davis Health Systems. 31 years of industry experience which include sales and operational positions. Substantial background successfully supporting Managed Print Services and Xerox Services accounts.

Bill Bennett, Client Manager (30 year with Xerox): Manages the entire sales cycle with assistance from numerous available resources-Manager, Specialists. Account General Manager. Provide support and related data industry trends, security related to our products and services and provide support of all of UC Davis' and UC Davis Health Systems. Day to day role is to identify, articulate and support products, software, services and solutions to best meet and customer's requirements while adhering to customer satisfaction goals.

Daria Lewis, Senior Client Manager (36 years with Xerox): Manages the entire sales cycle with accountability to engage specialist team members. Provide support and related data for industry trends, security related to our products and provide support of UC Irvine initiatives. Day to day role will identify, articulate, and implement products, solutions, and services to best suit customer requirements while adhering to increased customer satisfaction plans.

Marcia Quo-Schmidt, Senior Client Manager (36 years with Xerox)- Manages the entire sales cycle with accountability to engage specialist team members. Provides support and related data, industry trends, security related to our products and services. Identify and understand client's strategies and goals; then develop and implement solutions that align with their goals.

Martin Soto, Client Manager (15 years with Xerox): Manages the Xerox Relationship with UCLA. Works with Account General Manager, Sales Manager and Product Specialists. Provides support and related data, industry trends, security related to our products and services. Provides support of all of UCLA day to day role is to identify, articulate and support products, software, services and solutions to best meet and customer's requirements and expectations.

Bill Bennett, Client Manager (30 years with Xerox): Client Manger for UC Merced. 30 years supporting government and education with Xerox including UC Merced. Day to day role will identify, articulate, and implement products, solutions, and services to best suit customer requirements while adhering to increased customer satisfaction plans.

Marcia Quo-Schmidt, Senior Client Manager (36 years with Xerox): Account management and sales support for State/Local Government, and Higher Education to include UC Riverside. Her role is to educate and provide insight and knowledge of managed print services and products to help streamline their business processes. Identify and understand client's strategies and goals; then develop and implement solutions that align with their goals. Provide and maintain positive customer service with clients for continual partnership and growth.

Daria Lewis, Senior Client Manager (36 years with Xerox): Manages the Xerox relationship with UC San Diego's prints and document resource department, Imprints. Imprints has a staff of onsite technicians that provide service for roughly 400 Xerox MPD devices. My responsibilities include providing support and related data for industry trends, security related to our products and general support for UC San Diego initiatives.

Xerox® Office and Light Production Products



Industry Certifications

BLACK-AND-WHITE DEVICES	Print Driver / Server Environment Certifications								Application Certifications		
	WHQL	CITRIX® ⁰¹	IPV6 READY	BON-JOUR	GOOGLE CLOUD PRINT™	MOPRIA®	WI-FI DIRECT	APPLE® AIR-PRINT®	CERNER	MEDITECH (SEE PG. 3)	SAP
PRINTERS											
Xerox® B210	✓	✓	✓ ²	✓	✓	✓	✓	✓		✓	✓
Xerox® Phaser® 3330	✓	✓	✓	✓	✓ ²	✓	✓	✓	✓	✓	✓
Xerox® VersaLink® B400	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® B600/B610	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
MULTIFUNCTION PRINTERS											
Xerox® B205/215	✓	✓	✓ ²	✓	✓	✓	✓	✓		✓	✓
Xerox® WorkCentre® 3335/3345	✓	✓	✓	✓	✓ ³	✓	✓	✓	✓	✓	✓
Xerox® VersaLink® B405	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® B605/B615	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® B7025/B7030/B7035	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® WorkCentre® 5755 Factory Produced New Model	✓	✓	✓	✓							✓
Xerox® AltaLink® B8045/B8055/ B8065/B8075/B8090	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Xerox® PrimeLink B9100/B9110/B9125/B9136 ¹²	✓	✓	✓	✓	✓	✓			✓ ¹³	✓ ¹³	✓
Xerox® D95A/D110/D125 Copier/Printer	✓	✓							✓	✓	✓
Xerox® D110/D125 Printer	✓	✓							✓	✓	✓
Xerox® D136 Copier/Printer	✓	✓							✓	✓	✓
COLOR DEVICES											
PRINTERS											
Xerox® Phaser® 6510	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Xerox® VersaLink® C400	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® C500	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® C600	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® C7000	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® C8000	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Xerox® VersaLink® C9000	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
MULTIFUNCTION PRINTERS											
Xerox® WorkCentre® 6515	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Xerox® VersaLink® C405	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® C505	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® C605	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® VersaLink® C7020/C7025/C7030	✓	✓	✓	✓	✓	✓	✓ ⁶	✓	✓	✓	✓
Xerox® WorkCentre® 7535/7556 Factory Produced New Model	✓	✓	✓	✓							✓
Xerox® AltaLink® C8030/C8035/ C8045/C8055/C8070	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Xerox® Color C60/C70 Printer	✓	✓	✓ ²							✓	✓
Xerox® PrimeLink® C9065/C9070 Printer ¹²	✓	✓	✓	✓	✓	✓			✓	✓	✓
Xerox® WorkCentre® EC7836/EC7856	✓	✓	✓	✓					✓	✓	✓

BLACK-AND-WHITE DEVICES	Security Certifications		
	COMMON CRITERIA	FIPS 140-2	MCAFFEE® SECURITY

PRINTERS			
Xerox® B210			
Xerox® Phaser® 3330			
Xerox® VersaLink® B400		✓	
Xerox® VersaLink® B600/B610		✓	

MULTIFUNCTION PRINTERS			
Xerox® B205/215			
Xerox® WorkCentre® 3335/3345			
Xerox® VersaLink® B405	✓	✓	
Xerox® VersaLink® B605/B615	✓	✓	
Xerox® VersaLink® B7025/B7030/B7035	✓	✓	
Xerox® WorkCentre® 5755 Factory Produced New Model	✓	✓	
Xerox® AltaLink® B8045/B8055/ B8065/B8075/B8090	✓	✓	✓
Xerox® PrimeLink B9100/B9110/B9125/B9136 ¹²	✓ ¹³	✓	
Xerox® D95A/D110/D125 Copier/Printer	✓		
Xerox® D110/D125 Printer	✓		
Xerox® D136 Copier/Printer	✓	✓	

COLOR DEVICES

PRINTERS			
Xerox® Phaser® 6510			
Xerox® VersaLink® C400		✓	
Xerox® VersaLink® C500		✓	
Xerox® VersaLink® C600		✓	
Xerox® VersaLink® C7000		✓	
Xerox® VersaLink® C8000		✓	
Xerox® VersaLink® C9000		✓	

MULTIFUNCTION PRINTERS			
Xerox® WorkCentre® 6515			
Xerox® VersaLink® C405	✓	✓	
Xerox® VersaLink® C505	✓	✓	
Xerox® VersaLink® C605	✓	✓	
Xerox® VersaLink® C7020/C7025/C7030	✓	✓	
Xerox® WorkCentre® 7535/7556 Factory Produced New Model	✓	✓	
Xerox® AltaLink® C8030/C8035/ C8045/C8055/C8070	✓	✓	✓
Xerox® Color C60/C70 Printer	✓	✓	
Xerox® PrimeLink C9065/C9070 Printer ¹²	✓ ¹³	✓	
Xerox® WorkCentre® EC7836/EC7856	✓	✓	✓

Environmental Certifications			
ENERGY STAR®	BLUE ANGEL	ECOLOGO®	EPEAT® (MULTIPLE COUNTRIES) ⁷

✓	✓	✓	✓
✓	✓	✓	✓
✓ ⁵	✓	✓	✓ ⁵
✓	✓	✓	✓

✓ ³	✓ ³	✓ ³	✓ ³
✓ ⁸	✓	✓	✓ ⁸
✓	✓	✓	✓
✓	✓	✓	✓
✓	✓	✓	✓
		✓	
✓ ⁹		✓	✓ ⁹
✓			✓
✓			✓
✓			✓
✓			✓

✓	✓	✓	✓
✓ ⁵	✓	✓	✓ ⁵
✓ ⁵	✓	✓	✓ ⁵
✓ ⁵	✓	✓	✓ ⁵
✓	✓	✓	✓
✓	✓	✓	✓
✓	✓	✓	✓

✓	✓	✓	✓
✓ ⁵	✓	✓	✓ ⁵
✓	✓	✓	✓
✓	✓	✓	✓
✓	✓	✓	✓
		✓	
✓ ¹⁰	✓	✓	✓ ¹⁰
✓		✓	✓
✓	✓ ¹¹	✓	✓

¹ These products are Citrix Ready when using either the Xerox® Global Print Driver®, the product native print driver or the Citrix universal driver; ² Device is compliant / tested, but has not been formerly certified. ³ Xerox B215 Multifunction Printer only; ⁴ XenApp 5.0 and up; ⁵ DN configuration only; ⁶ Requires optional wireless network adapter; ⁷ All products certified in the U.S. EPEAT-certified products vary by country in Belgium, Canada, Denmark, Finland, France, Germany, Holland, Luxembourg, Norway, Sweden, Switzerland and the U.K. Visit www.epeat.net for information regarding country-specific EPEAT certifications; ⁸ Xerox® WorkCentre® 3345 only; ⁹ Xerox® AltaLink® B8065/B8075/B8090 only; ¹⁰ Xerox® AltaLink® C8030 220V not Energy Star® or EPEAT® certified; ¹¹ Certification in progress; ¹² Xerox Integrated Server; ¹³ Undergoing evaluation.

PRINT DRIVER / SERVER ENVIRONMENT CERTIFICATIONS

Microsoft® WHQL Certification

Windows Hardware Quality Labs testing involves running a series of tests on third-party hardware or software, and then submitting the log files from these tests to Microsoft for review. Xerox® products that are Windows Hardware Quality Labs (WHQL) certified comply with Microsoft standards and ensure seamless compatibility with Microsoft Windows environments.

Citrix® Certification

Citrix Systems is an American multinational software and services company that specializes in virtualization and remote access software for delivering applications over a network and the Internet. Xerox is part of the Citrix ready program, which allows vendors to perform a self evaluation of its product against a set of metrics outlined by Citrix. Once the product passes certification, Xerox pays an annual fee for having its certified products listed on the Citrix website as well as the right to use its logo. This certification ensures that a product using Citrix software will function as expected in a remote environment.

IPv6 Ready

Internet Protocol version 6 (IPv6) is a relatively new protocol for routing network traffic and identifying network-connected devices. IPv6 will be phased in over many years as the next-generation replacement for the global IPv4 standard. Because printers and multifunction printers comprise a sizable percentage of the world's networked devices, Xerox is transitioning its products' capabilities to be IPv6-compatible.

Bonjour®

Bonjour is Apple Inc.'s trade name for its implementation of zero-configuration networking, a service discovery protocol. Bonjour enables automatic discovery of devices such as printers, other computers, and the services that those devices offer on IP networks using industry standard IP protocols.

Google Cloud Print™

Google Cloud Print is a simple mobile printing solution for mobile workers that can't count on having access to the same printer or MFP all the time; or do not have the appropriate print driver software for the printer or MFP that is available. Google Cloud Print enabled printers and MFPs allow mobile workers to securely and directly connect and register with the Google Cloud Print service, so it's always available. No need to install and maintain print drivers or additional software.

Mopria®

Mopria is an acronym derived from the Mobile Print Alliance. The charter of this alliance of printer manufacturers is to create simple wireless printing from smartphones, tablets, and other mobile devices. Mopria printing does not require any driver installation or software download on these devices. Mopria Print functionality will be embedded in phones, tablets or other mobile devices and there is no set-up required. When mobile device users have access to a Mopria-certified printer, they will be able to effortlessly discover and print to this printer. Mopria will be initially supported for users of Android™ Kit Kat (4.4)-based devices using a free plug-in available in the Google Play™ store.

Wi-Fi Direct Certification

This certification lets you print from your mobile device without having to connect to a network. Adding the optional wireless USB adapter enables this connection, and allows for both an Ethernet connection and Wi-Fi Direct connection to be enabled at the same time.

Apple® AirPrint

Apple AirPrint is a driverless printing technology and was introduced with iOS® version 4.2 in November 2010. It enables Apple iOS devices including the iPhone®, iPad®, iPod touch®, and even Mac OS® X computers to print with no need to install drivers or download software. AirPrint uses well-established, familiar technologies already in use today, such as Bonjour, IPP, PDF and JPEG. AirPrint will likely continue to evolve to add new features and functionality, however, the basic operation of AirPrint will remain constant, in that it requires only a few steps to ensure it works as it was designed to do.

APPLICATION CERTIFICATIONS

Cerner Certification

Cerner is the leading U.S. supplier of healthcare information technology solutions that optimize clinical and financial outcomes. Around the world, health organizations ranging from single-doctor practices to entire countries turn to Cerner for their powerful yet intuitive solutions. Cerner offers clients a dedicated focus on healthcare, an end-to-end solution and service portfolio, and proven market leadership. Xerox pays Cerner for product certification, which is a 6-8 week process after the product is received in Kansas City. Once certified, Cerner lists the product on its internal customer website and sends Xerox a certificate. This certification allows Xerox to participate in customer bids where Cerner Certification is a requirement. Xerox also provides a product, including all supplies and service, to Cerner until that product is at end of life. Cerner Certification is important to a customer's IT staff as this allows them the comfort of having 24/7 support 365 days a year, through the Cerner help desk. Cerner provides this support as part of their HIS package. For example, a hospital can call and report a downed printer in the Emergency Room at 3 a.m. and receive remote support for that printer.

MEDITECH Certification

Medical Information Technology, Inc. (MEDITECH) is a leading provider of integrated software solutions for healthcare organizations worldwide. This certification validates that Xerox® devices are fully compatible with MEDITECH's MAGIC operating system: a health information system that provides a structured and easy-to-use programming language to more than 1,500 healthcare organizations worldwide. With this certification Xerox continues to achieve noteworthy healthcare industry praise for its award-winning line of devices and it allows Xerox to participate in customer bids where MEDITECH Certification is a requirement. These certified devices are then fully supported by MEDITECH help desk technicians 24/7, 365 days a year, giving their clients and ours the assurance that support will be available at all times.

SAP Certification

Xerox, together with SAP through our Gold-level membership in the SAP Printer Vendor Program, provides seamless connectivity between SAP systems and your Xerox® printers and MFPs. And as an SAP customer you benefit from having SAP-certified Xerox® device types available right from SAP's online delivery model. Whether you are using an existing Xerox® product or plan to upgrade, you can be assured that you will have printing continuity within your SAP environment. You also have the peace of mind knowing that you can contact SAP for support regarding any device type issues. And Xerox has a direct link to SAP that allows us to keep our device types current and in line with SAP release updates. SAP-certified device types are available for the legacy R/3 system and newer ERP releases all the way up to current SAP offerings.

SECURITY CERTIFICATIONS

Common Criteria Certification

Common Criteria Certification provides independent, objective validation of the reliability, quality, and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria (aka ISO 15408) sets specific information assurance goals, including strict levels of integrity, confidentiality, and availability for systems and data, accountability at the individual level, and assurance that all goals are met. Common Criteria Certification is a requirement for hardware and software devices used by the federal government on national security systems.

FIPS 140-2

All hardware and software components that are used by government and other key industries for the purpose of collecting, storing, transferring, sharing and disseminating sensitive but unclassified information are required to be FIPS 140-2 certified. FIPS 140 is a series of coordinated requirements issued by the National Institute of Standards and Technology (NIST) to validate the product's level of security depending on its intended use.

McAfee® Security

Built-in McAfee security provides protection against intrusion from within Xerox® MFPs built on Xerox® ConnectKey® Technology. Two levels of protection are offered.

McAfee Enhanced Security is standard and allows only an approved, predefined list of applications, code and software files to run on the device. This McAfee agent is Xerox factory installed and it monitors in the background for any changes to Xerox factory default system applications used to operate the device.

McAfee Integrity Control is an optional, commercial application that supports a higher level of whitelisting and change control or dynamic whitelisting. This protects the device's executable files from tampering and identifies trusted sources, controls what can change, who can change and when it can change.

ENVIRONMENTAL COMPLIANCE

ENERGY STAR®

With the goals of reducing energy consumption and greenhouse gas emission, ENERGY STAR is a voluntary program sponsored by the United States Environment Protection Agency. Products carrying the label are certified for matching or beating federal energy conservation standards.

Blue Angel

Based in Germany, Blue Angel was the world's first certification for environmental friendliness. Its purposes are to promote ecological awareness and to guide environmentally conscious consumers to the most ecologically sound products.

ECOLOGO®





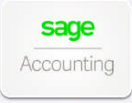


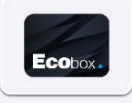
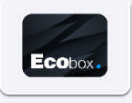






Canada's ECOLOGO certification is especially stringent. This program mandates strict environmentally conscious requirements must be met throughout the life-cycle of the product, and it must also meet performance requirements when compared to its closest alternatives.

EPEAT®






EPEAT (multiple countries) is a global registry for environmentally friendly electronics for purchasers, manufacturers, resellers and others wanting to find and promote environmentally preferable products. EPEAT uses a self-declaration and rigorous verification system to ensure the products conform to the established criteria. Once products are added to the registry, EPEAT may use independent experts to verify that the products meet the selected criteria as claimed. All Xerox® products listed in this document are EPEAT-certified in the U.S. Various products are also certified in additional countries. For more information, go to www.epeat.net.

Xerox App Gallery

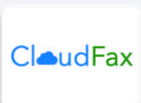



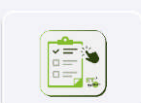
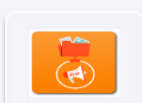

Business

 Connect for Concur Xerox Corporation	 Connect for DocuSign Xerox Corporation	 Connect for Exchange Online Xerox Corporation
 Connect for NetSuite Xerox Corporation	 Connect for Sage Accounting Xerox Corporation	 Connect For Salesforce App Xerox Corporation
 Connect for XMPie Xerox Corporation Free	 EcoBox DE DK FI UK SE TBC Solutions	 EcoBox France TBC Solutions
 ET-Badge EtiQube	 MC Counter MC System srl	 QuickBooks Online Xerox Corporation
 Scanning App for DocuShare Xerox Corporation Free	 Yooz Connect Free e-Cervo Free	 Yooz Connect™ e-Cervo

Cloud Storage

 Connect 2.0 for Box Xerox Corporation	 Connect 2.0 for Google Drive Xerox Corporation	 Connect 2.0 for Microsoft Office 365 Xerox Corporation
 Connect 2.0 for Microsoft OneDrive Xerox Corporation	 Connect For Evernote Xerox Corporation	

Communication

 CloudFax Connector JustTech	 Connect for RMail Xerox Corporation	 eGoldFax Connector JustTech
 Email Connect JustTech Free	 ET-Survey EtiQube	 Mywork Digital Communication MyWorkPlatform
 Scan to Cloud Email Xerox Corporation Free		

Education



Book2Go
e-dox AG



Connect for Blackboard
Xerox Corporation



Connect for Moodle
Xerox Corporation



Remark Test Grading
Xerox Corporation



Xerox Proofreader
Xerox Corporation

General



Ask
Xerox Emirates L.L.C.
Free



Billboard Lite
Vision-e



Billboard Pro
Vision-e



OVH Fax Pro
TBC Solutions



Scan to Zoho
TBC Solutions



Xerox Audio Documents
Xerox Corporation



Xerox Note Converter
Xerox Corporation



Xerox Translate and Print
Xerox Corporation



Сервисная организация
Xerox Russia
Free

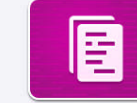
Legal



Connect for Clio
Xerox Corporation



Connect for iManage
Xerox Corporation



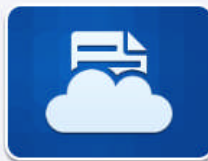
Xerox® Auto-Redaction
Xerox Corporation

Medical



Share Patient Information
Xerox Corporation
Free

Mobile Solutions



@PrintByXerox
Xerox Corporation
Free



QR Code
Xerox Corporation
Free

Productivity



AIDA
Technology & Cognition LAB



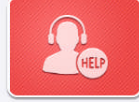
Amazon WorkDocs
MyWorkPlatform



CapturePoint XAG
Process Fusion Inc.



Forms Manager
Xerox Corporation



Helpdesk Connector
Xerox Russia
Free



MDRL
TBC Knowledge Management



Mywork E-Sign
MyWorkPlatform



Quick Link
Xerox Corporation
Free



Wetransfer
MyWorkPlatform

Utilities



Support Assistant 3.0
Xerox Corporation
Free



Xerox® App Gallery
Xerox Corporation
Free

Xerox Accessibility Section 508 Conformance Report

Voluntary Product Accessibility Template® (VPAT®) V2.0

Xerox® VersaLink® C7020/C7025/C7030 MFP



Learn more about Xerox and Section 508 at our website:

www.xerox.com/Section508

Summary Table – Voluntary Product Accessibility Template® (VPAT®)

Criteria	Conformance Level	Remarks and explanations
Chapter 3: Functional Performance Criteria	Supports	The product is compliant with Chapter 3
Chapter 4: Hardware	Supports with exceptions	Compliant with minor exceptions concerning volume and input controls
Chapter 5: Software	Not applicable	The product does not support the software criteria set forth
Chapter 6: Support Documentation and Services	Supports	The centralization of documentation, training, and support services for most Xerox products allows us to achieve compliance across the corporation.

Software Version Evaluated: 1.11.12 Driver SW.version:5.528.5.0

Accessories Included in Evaluation: external keyboard, narrator (inbuilt in windows), and headset

Evaluation Methods Used: testing based on general product knowledge, similar to another evaluated product, and testing with assistive technologies

Chapter 3: Functional Performance Criteria (FPC)

Criteria	Conformance Level	Remarks and explanations
302.1 Without Vision	Supports	Person without vision can make use of the rocker switch behind the door to power on/off the machine. Also, supported with XCA as the speech output can be directed to the individuals
302.2 With Limited Vision	Supports	Person with limited vision is able to perform all the operations available based on limited vision of 20/70
302.3 Without Perception of Color	Supports	At least one mode of operation that does not require
302.4 Without Hearing	Supports	One mode of operation that does not require user hearing is available
302.5 With Limited Hearing	Supports	One mode of operation that does not require user limited hearing is available
302.6 Without Speech	Not applicable	Speech is not required for this product
302.7 With Limited Manipulation	Supports	Fine motor control is for where adjustment is associated with things like dials and sliders. Where sliders are used to adjust things like copy darkness/lightness the slider will work as a single touch as well as touch and slide, therefore can be considered to support, as it does not require fine motor control. Input of destination can be via preconfigured selection from address book – no need to type in destination.
302.8 With Limited Reach and Strength	Supports	At least one mode of operation that does not require limited reach and limited strength is available
302.9 With limited Language, Cognitive, and Learning Abilities	Supports	Features are provided for individuals with limited cognitive, language, and learning abilities for simpler and easier use

Chapter 4: Hardware

Criteria	Conformance Level	Remarks and explanations
402 Closed Functionality		
402.1 General		
402.2 Speech-Output Enabled		
402.2.1 Information Displayed On-Screen	Not applicable	This product does not have a display screen
402.2.2 Transactional Outputs	Not applicable	There is no speech output
402.2.3 Speech Delivery Type and Coordination	Not applicable	There is no speech output
402.2.4 User Control	Not applicable	There is no voice output.
402.2.5 Braille Instructions	Not applicable	There is no speech output
402.3 Volume		
402.3.1 Private Listening	Not applicable	There is no voice output.
402.3.2 Non-private Listening	Not applicable	There is no voice output.
402.4 Characters on Display Screens	Supports with exceptions	All text is sans serif but text is 4mm

Criteria	Conformance Level	Remarks and explanations
402.5 Characters on Variable Message Signs	Not applicable	Device does not employ variable message signs as defined in section 7, which relates to signage such as exit signs.
403 Biometrics		
403.1 General	Not applicable	Biometric forms are not used.
404 Preservation of Information Provided for Accessibility		
404.1 General	Not applicable	The device does not transmit or conduct information or communication.
405 Privacy		
405.1 General	Supports	The product provides same degree of privacy of input and output for all users
406 Standard Connections		
406.1 General	Supports	The data connections are such as fax line. Internet cable are industry standard formats
407 Operable Parts		
407.2 Contrast	Supports	Characters and symbols is contrast visually from background surfaces with either light characters on a dark background.
407.3 Input Controls		
407.3.1 Tactilely Discernible	Supports	Touch screen is not tactilely discernible. Power control is discernible based on using the rocker switch behind door. UI controls are discernible for power (home button can by differentiated compared to power button)
407.3.2 Alphabetic Keys	Not applicable	The product does not include any mechanically operated controls or keys
407.3.3 Numeric Keys	Not applicable	A 12-key ascending or descending keypad layout is not provided.
407.4 Key Repeat	Not applicable	Key repeat is not supported.
407.5 Timed Response	Supports with exceptions	Alert message appears visually in the LUI to provide the timed response but not by sound.
407.6 Operation	Supports	Operations which are available with the printer are easy to operate without any difficulties.
407.7 Tickets, Fare Cards, and Keycards	Not applicable	Tickets, Fare card or keycard is not used in product
407.8 Reach Height and Depth		
407.8.1 Vertical Reference Plane	Supports	At least one of each type of operable part of stationary ICT at a height conforming to 407.8.2 or 407.8.3 is available
407.8.1.1 Vertical Plane for Side Reach	Supports	Where a side reach is provided, the vertical reference plane is 48 inches (1220 mm) long minimum.

Criteria	Conformance Level	Remarks and explanations
407.8.1.2 Vertical Plane for Forward Reach.	Supports	Where a forward reach is provided, the vertical reference plane is 30 inches (760 mm) long minimum
407.8.2 Side Reach	Supports	Where a side reach requires a reach over a portion of the ICT, the height of that portion of the ICT is 34 inches (865 mm) maximum.
407.8.2.1 Unobstructed Side Reach	Supports	Where the operable part is located 10 inches (255 mm) or less beyond the vertical reference plane, the operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor.
407.8.2.2 Obstructed Side Reach	Supports	All operable controls are within specification.
407.8.3 Forward Reach	Supports	Where a forward reach allows a reach over a portion of the ICT, the height of that portion of the ICT shall be 34 inches (865 mm) maximum
407.8.3.1 Unobstructed Forward Reach	Supports	The operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor
407.8.3.2 Obstructed Forward Reach	Supports	Supports maximum allowable forward reach to an operable part is 25inches
407.8.3.2.1 Operable Part Height for ICT with Obstructed Forward Reach	Supports	All operable parts are within specification
407.8.3.2.2 Knee and Toe Space under ICT with Obstructed Forward Reach	Not applicable	No obstructed forward reach.
408 Display Screens		
408.2 Visibility	Supports	The printers LUI is adjustable up and down so user is able to view the screen even if it is 40 inches above the floor.
408.3 Flashing	Supports	The power key LED conforms
409 Status Indicators		
409.1 General	Supports	Status indicators are provided visually and by sound
410 Color Coding		
410.1 General	Supports	Jam zones are identified by number as well as color
411 Audible Signals		
411.1 General	Supports	Audible signal ex. Job completion gives an audio signal and also gives in text message in LUI
412 ICT with Two-Way Voice Communication		
412.2 Volume Gain		
412.2.1 Volume Gain for Wireline Telephones	Not applicable	This product does not use analog or digital wireline telephones.

Criteria	Conformance Level	Remarks and explanations
412.2.2 Volume Gain for Non-Wireline ICT	Not applicable	The device does not support bi-directional voice communication over a telephone line.
412.3 Interference Reductions and Magnetic Coupling		
412.3.1 Wireless Handsets	Not applicable	The product does not produce electromagnetic fields.
412.3.2 Wireline Handsets	Not applicable	The product does not produce electromagnetic fields.
412.4 Digital Encoding of Speech	Not applicable	This product does not support digital encoding of speech
412.5 Real-time Text Functionality	Not applicable	Real-time text functionality is not present.
412.6 Called ID	Not applicable	Caller ID and/or similar telecommunications are not present.
412.7 Video Communication	Not applicable	The product is not a video or multi-media product.
413 Closed Caption Processing Technologies		
413.1.1 Decoding and Display of Closed Captions	Not applicable	The product is not a video or multi-media product.
413.1.2 Pass-Through of Closed Caption Data	Not applicable	The device does not transmit or conduct information or communication.
414 Audio Description Processing Technologies		
414.1.1 Digital Television Tuners	Not applicable	The product is not a video or multi-media product.
414.1.2 Other ICT	Not applicable	The product is not a video or multi-media product.
415 User Controls for Captions and Audio Descriptions		
415.1.1 Caption Controls	Not applicable	The product is not a video or multi-media product.
415.1.2 Audio Description Controls	Not applicable	The product is not a video or multi-media product.

Chapter 6 Support Documentation and Services

Criteria	Conformance Level	Remarks and explanations
601.1 Scope		
602 Support Documentation		
602.2 Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide
602.3 Electronic Support Documentation	Supports	Website provides guide to use the device
602.4 Alternate Formats for Non-Electronic Support Documentation	Supports	User guide is provided as an E-book to the customer
603 Support Services		
603.2 Information on Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide

Criteria	Conformance Level	Remarks and explanations
603.3 Accommodation of Communication Needs	Not applicable	Customer support service contact details are available in the user guide and also on the website. Specific support for persons with disabilities not provided

What is the Voluntary Product Accessibility Template (VPAT)?

The purpose of the Voluntary Product Accessibility Template is to assist Federal contracting officials in making preliminary assessments regarding the availability of commercial Electronic and Information Technology products and services with features that support accessibility.

The first table of the Template provides a summary view of the Section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. In the subsequent tables, the first column contains the numbered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

For additional information on these and other accessories, contact your Xerox sales representative or call 1-800-ASK-XEROX (1-800-275-9376).

© 2017 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design®, and VersaLink® are trademarks of Xerox Corporation in the United States and/or other countries. BR22162

Other company trademarks are also acknowledged.

Document Version: 1.0 (January 2017).

Voluntary Product Accessibility Template® and VPAT® are registered service marks of the Information Technology Industry Council (ITI).

Xerox Accessibility Section 508 Conformance Report

Voluntary Product Accessibility Template® (VPAT®) V2.0

Xerox® VersaLink® B7025/B7030/B7035 MFP



Learn more about Xerox and Section 508 at our website:

www.xerox.com/Section508

Summary Table – Voluntary Product Accessibility Template® (VPAT®)

Criteria	Conformance Level	Remarks and explanations
Chapter 3: Functional Performance Criteria	Supports	The product is compliant with Chapter 3
Chapter 4: Hardware	Supports with exceptions	Compliant with a minor exception concerning input controls, status indicators, and volume
Chapter 5: Software	Not applicable	The product does not support the software criteria set forth
Chapter 6: Support Documentation and Services	Supports	The centralization of documentation, training, and support services for most Xerox products allows us to achieve compliance across the corporation

Software Version Evaluated: Firmware version:1.10.9

Accessories Included in Evaluation: none

Evaluation Methods Used: Testing based on general product knowledge and similar to another evaluated product

Chapter 3: Functional Performance Criteria (FPC)

Criteria	Conformance Level	Remarks and explanations
302.1 Without Vision	Supports	At least one mode of operation that does not require user vision is available
302.2 With Limited Vision	Supports	At least one mode of operation that enables users to make use of limited vision is available
302.3 Without Perception of Color	Supports	At least one mode of operation that does not require user perception of color is available
302.4 Without Hearing	Supports	One mode of operation that does not require user hearing is available
302.5 With Limited Hearing	Supports	One mode of operation that does not require user limited hearing is available
302.6 Without Speech	Not applicable	Speech is not required for this product
302.7 With Limited Manipulation	Supports	At least one mode of operation that does not require fine motor control or simultaneous manual operations is available
302.8 With Limited Reach and Strength	Supports	At least one mode of operation that does not require limited reach and limited strength is available
302.9 With limited Language, Cognitive, and Learning Abilities	Supports	Features are provided for individuals with limited cognitive, language, and learning abilities for simpler and easier use

Chapter 4: Hardware

Criteria	Conformance Level	Remarks and explanations
402 Closed Functionality		
402.1 General		
402.2 Speech-Output Enabled		
402.2.1 Information Displayed On-Screen	Not applicable	This product does not have a display screen
402.2.2 Transactional Outputs	Not applicable	There is no transactional output
402.2.3 Speech Delivery Type and Coordination	Not applicable	There is no speech output
402.2.4 User Control	Not applicable	There is no voice output
402.2.5 Braille Instructions	Not applicable	There is no speech output
402.3 Volume		
402.3.1 Private Listening	Not applicable	There is no voice output
402.3.2 Non-private Listening	Not applicable	There is no voice output
402.4 Characters on Display Screens	Supports with exceptions	At least one mode of characters displayed on the screen is in sans serif font is available but text is 4mm
402.5 Characters on Variable Message Signs	Not applicable	This product does not have variable message signs
403 Biometrics		

Criteria	Conformance Level	Remarks and explanations
403.1 General	Not applicable	Biometric forms are not used
404 Preservation of Information Provided for Accessibility		
404.1 General	Not applicable	The device does not transmit or conduct information or communication
405 Privacy		
405.1 General	Supports	The same degree of privacy of input and output is provided to all individuals
406 Standard Connections		
406.1 General	Supports	At least one type of connection (fax line and internet cable) conform to industry standard non-priority format
407 Operable Parts		
407.2 Contrast	Supports	The product provides keys and controls with contrast visually from background surfaces
407.3 Input Controls		
407.3.1 Tactilely Discernible	Supports	Input controls are operable by touch and tactilely discernible without activation
407.3.2 Alphabetic Keys	Not applicable	The product does not include any mechanically operated controls or keys
407.3.3 Numeric Keys	Not applicable	A 12-key ascending or descending keypad layout is not provided
407.4 Key Repeat	Not applicable	Key repeat is not supported
407.5 Timed Response	Supports with exceptions	Alert provided only visually but not by sound
407.6 Operation	Supports	Controls do not require simultaneous use of two hands, and the force to activate hand-operated controls is less than 5 lbs
407.7 Tickets, Fare Cards, and Keycards	Not applicable	Tickets, Fare card or keycard is not used in product
407.8 Reach Height and Depth		
407.8.1 Vertical Reference Plane	Supports	At least one of each type of operable part of stationary ICT at a height conforming to 407.8.2 or 407.8.3 is available
407.8.1.1 Vertical Plane for Side Reach	Supports	Where a side reach is provided, the vertical reference plane is 48 inches (1220 mm) long minimum
407.8.1.2 Vertical Plane for Forward Reach.	Supports	Where a forward reach is provided, the vertical reference plane is 30 inches (760 mm) long minimum
407.8.2 Side Reach	Supports	Where a side reach requires a reach over a portion of the ICT, the height of that portion of the ICT is 34 inches (865 mm) maximum
407.8.2.1 Unobstructed Side Reach	Supports	Where the operable part is located 10 inches (255 mm) or less beyond the vertical reference plane, the operable part is 48 inches (1220 mm) high maximum

Criteria	Conformance Level	Remarks and explanations
		and 15 inches (380 mm) high minimum above the floor
407.8.2.2 Obstructed Side Reach	Supports	All operable controls are within specification
407.8.3 Forward Reach	Supports	Where a forward reach allows a reach over a portion of the ICT, the height of that portion of the ICT shall be 34 inches (865 mm) maximum
407.8.3.1 Unobstructed Forward Reach	Supports	The operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor
407.8.3.2 Obstructed Forward Reach	Supports	Supports maximum allowable forward reach to an operable part is 25inches
407.8.3.2.1 Operable Part Height for ICT with Obstructed Forward Reach	Supports	All operable parts are within specification
407.8.3.2.2 Knee and Toe Space under ICT with Obstructed Forward Reach	Not applicable	There are no operable controls
408 Display Screens		
408.2 Visibility	Supports	At least one display screen is visible from a point located 40inches above floor space
408.3 Flashing	Supports	This product supports no more than three flashes in any one-second period
409 Status Indicators		
409.1 General	Supports	Status indicators are discernible visually and by touch or sound
410 Color Coding		
410.1 General	Supports	Color coding and additional means of unique identification (e.g., text and symbols) are used
411 Audible Signals		
411.1 General	Supports	Audible signals and additional means of unique identification (e.g., cues) are used
412 ICT with Two-Way Voice Communication		
412.2 Volume Gain		
412.2.1 Volume Gain for Wireline Telephones	Not applicable	This product does not use analog or digital wireline telephones
412.2.2 Volume Gain for Non-Wireline ICT	Not applicable	The device does not support bi-directional voice communication over a telephone line
412.3 Interference Reductions and Magnetic Coupling		
412.3.1 Wireless Handsets	Not applicable	The product does not produce electromagnetic fields
412.3.2 Wireline Handsets	Not applicable	The product does not produce electromagnetic fields
412.4 Digital Encoding of Speech	Not applicable	This product does not support digital encoding of speech
412.5 Real-time Text Functionality	Not applicable	This product does not support real-time functionality
412.6 Called ID	Not applicable	Caller ID and/or similar telecommunications are not present

Criteria	Conformance Level	Remarks and explanations
412.7 Video Communication	Not applicable	The product is not a video or multi-media product
413 Closed Caption Processing Technologies		
413.1.1 Decoding and Display of Closed Captions	Not applicable	The product is not a video or multi-media product
413.1.2 Pass-Through of Closed Caption Data	Not applicable	The device does not transmit or conduct information or communication
414 Audio Description Processing Technologies		
414.1.1 Digital Television Tuners	Not applicable	The product is not a video or multi-media product
414.1.2 Other ICT	Not applicable	The product is not a video or multi-media product
415 User Controls for Captions and Audio Descriptions		
415.1.1 Caption Controls	Not applicable	The product is not a video or multi-media product
415.1.2 Audio Description Controls	Not applicable	The product is not a video or multi-media product

Chapter 6 Support Documentation and Services

Criteria	Conformance Level	Remarks and explanations
601.1 Scope		
602 Support Documentation		
602.2 Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide
602.3 Electronic Support Documentation	Supports	Website provides user guide
602.4 Alternate Formats for Non-Electronic Support Documentation	Supports	User guide is provided as an E-book to the customer
603 Support Services		
603.2 Information on Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide
603.3 Accommodation of Communication Needs	Not applicable	Customer support service contact details are available in the user guide and also on website. Specific support for persons with disability is not provided

What is the Voluntary Product Accessibility Template (VPAT)?

The purpose of the Voluntary Product Accessibility Template is to assist Federal contracting officials in making preliminary assessments regarding the availability of commercial Electronic and Information Technology products and services with features that support accessibility.

The first table of the Template provides a summary view of the Section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. In the subsequent tables, the first column contains the numbered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

For additional information on these and other accessories, contact your Xerox sales representative or call 1-800-ASK-XEROX (1-800-275-9376).

© 2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR22162
Other company trademarks are also acknowledged.
Document Version: 1.0 (January 2017).

Voluntary Product Accessibility Template® and VPAT® are registered service marks of the Information Technology Industry Council (ITI).

Xerox Accessibility Section 508 Conformance Report

Voluntary Product Accessibility Template® (VPAT®) V2.0

Xerox® VersaLink® B405 MFP



Learn more about Xerox and Section 508 at our website:

www.xerox.com/Section508

Summary Table – Voluntary Product Accessibility Template® (VPAT®)

Criteria	Conformance Level	Remarks and explanations
Chapter 3: Functional Performance Criteria	Supports	The product is compliant with Chapter 3.
Chapter 4: Hardware	Supports with exceptions	Compliant with minor exceptions concerning volume, input controls, and status indicators
Chapter 5: Software	Not applicable	The product does not support the software criteria set forth
Chapter 6: Support Documentation and Services	Supports	The centralization of documentation, training, and support services for most Xerox products allows us to achieve compliance across the corporation.

Software Version Evaluated: Firmware version: 1.0.15

Evaluation Methods Used: Testing based on general product knowledge, similar to another evaluated product

Chapter 3: Functional Performance Criteria (FPC)

Criteria	Conformance Level	Remarks and explanations
302.1 Without Vision	Supports	At least one mode of operation that does not require user vision is available
302.2 With Limited Vision	Supports	At least one mode of operation that enables users to make use of limited vision is available
302.3 Without Perception of Color	Supports	At least one mode of operation that does not require user perception of color is available
302.4 Without Hearing	Supports	One mode of operation that does not require user hearing is available
302.5 With Limited Hearing	Supports	One mode of operation that does not require user limited hearing is available
302.6 Without Speech	Not applicable	Speech is not required for this product
302.7 With Limited Manipulation	Supports	At least one mode of operation that does not require fine motor control or simultaneous manual operations is available
302.8 With Limited Reach and Strength	Supports	At least one mode of operation that does not require limited reach and limited strength is available
302.9 With limited Language, Cognitive, and Learning Abilities	Supports	Features are provided for individuals with limited cognitive, language, and learning abilities for simpler and easier use

Chapter 4: Hardware

Criteria	Conformance Level	Remarks and explanations
402 Closed Functionality		
402.1 General		
402.2 Speech-Output Enabled		
402.2.1 Information Displayed On-Screen	Not applicable	This product does not have a display screen
402.2.2 Transactional Outputs	Not applicable	There is no transactional output
402.2.3 Speech Delivery Type and Coordination	Not applicable	There is no speech output
402.2.4 User Control	Not applicable	There is no voice output.
402.2.5 Braille Instructions	Not applicable	There is no speech output
402.3 Volume		
402.3.1 Private Listening	Not applicable	There is no voice output.
402.3.2 Non-private Listening	Not applicable	There is no voice output.
402.4 Characters on Display Screens	Supports with exceptions	All text is Sans Serif but text is 4mm
402.5 Characters on Variable Message Signs	Not applicable	This product does not have variable message signs
403 Biometrics		

Criteria	Conformance Level	Remarks and explanations
403.1 General	Not applicable	Biometric forms are not used.
404 Preservation of Information Provided for Accessibility		
404.1 General	Not applicable	The device does not transmit or conduct information or communication.
405 Privacy		
405.1 General	Supports	The same degree of privacy of input and output is provided to all individuals
406 Standard Connections		
406.1 General	Supports	At least one type of connection conform to industry standard non-priority format.
407 Operable Parts		
407.2 Contrast	Supports	The product provides keys and controls with contrast visually from background surfaces
407.3 Input Controls		
407.3.1 Tactilely Discernible	Supports	Input controls are operable by touch and tactilely discernible without activation.
407.3.2 Alphabetic Keys	Not applicable	The product does not include any mechanically operated controls or keys
407.3.3 Numeric Keys	Not applicable	A 12-key ascending or descending keypad layout is not provided.
407.4 Key Repeat	Not applicable	Key repeat is not supported.
407.5 Timed Response	Supports with exceptions	Alert message appears visually in the LUI to provide the timed response but not by sound
407.6 Operation	Supports	Controls do not require simultaneous use of two hands, and the force to activate hand-operated controls is less than 5 lbs.
407.7 Tickets, Fare Cards, and Keycards	Not applicable	Tickets, Fare card or keycard is not used in product
407.8 Reach Height and Depth		
407.8.1 Vertical Reference Plane	Supports	At least one of each type of operable part of stationary ICT at a height conforming to 407.8.2 or 407.8.3 is available
407.8.1.1 Vertical Plane for Side Reach	Supports	Where a side reach is provided, the vertical reference plane is 48 inches (1220 mm) long minimum.
407.8.1.2 Vertical Plane for Forward Reach.	Supports	Where a forward reach is provided, the vertical reference plane is 30 inches (760 mm) long minimum
407.8.2 Side Reach	Supports	Where a side reach requires a reach over a portion of the ICT, the height of that portion of the ICT is 34 inches (865 mm) maximum.
407.8.2.1 Unobstructed Side Reach	Supports	Where the operable part is located 10 inches (255 mm) or less beyond the vertical reference plane, the operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor.

Criteria	Conformance Level	Remarks and explanations
407.8.2.2 Obstructed Side Reach	Supports	All operable controls are within specification.
407.8.3 Forward Reach	Supports	Where a forward reach allows a reach over a portion of the ICT, the height of that portion of the ICT shall be 34 inches (865 mm) maximum
407.8.3.1 Unobstructed Forward Reach	Supports	The operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor
407.8.3.2 Obstructed Forward Reach	Supports	Supports maximum allowable forward reach to an operable part is 25inches
407.8.3.2.1 Operable Part Height for ICT with Obstructed Forward Reach	Supports	All operable parts are within specification
407.8.3.2.2 Knee and Toe Space under ICT with Obstructed Forward Reach	Not applicable	There are no operable controls
408 Display Screens		
408.2 Visibility	Supports	At least one display screen is visible from a point located 40inches above floor space
408.3 Flashing	Supports	This product supports no more than three flashes in any one-second period.
409 Status Indicators		
409.1 General	Supports with exceptions	Status indicators provide visual only
410 Color Coding		
410.1 General	Supports	Color coding and additional means of unique identification (e.g., text and symbols) are used.
411 Audible Signals		
411.1 General	Supports	Audible signals and additional means of unique identification (e.g., cues) are used.
412 ICT with Two-Way Voice Communication		
412.2 Volume Gain		
412.2.1 Volume Gain for Wireline Telephones	Not applicable	This product does not use analog or digital wireline telephones.
412.2.2 Volume Gain for Non-Wireline ICT	Not applicable	The device does not support bi-directional voice communication over a telephone line.
412.3 Interference Reductions and Magnetic Coupling		
412.3.1 Wireless Handsets	Not applicable	The product does not produce electromagnetic fields.
412.3.2 Wireline Handsets	Not applicable	The product does not produce electromagnetic fields.
412.4 Digital Encoding of Speech	Not applicable	This product does not support digital encoding of speech
412.5 Real-time Text Functionality	Not applicable	This product does not support real-time functionality
412.6 Called ID	Not applicable	Caller ID and/or similar telecommunications are not present.
412.7 Video Communication	Not applicable	The product is not a video or multi-media product.
413 Closed Caption Processing Technologies		

Criteria	Conformance Level	Remarks and explanations
413.1.1 Decoding and Display of Closed Captions	Not applicable	The product is not a video or multi-media product.
413.1.2 Pass-Through of Closed Caption Data	Not applicable	The device does not transmit or conduct information or communication.
414 Audio Description Processing Technologies		
414.1.1 Digital Television Tuners	Not applicable	The product is not a video or multi-media product.
414.1.2 Other ICT	Not applicable	The product is not a video or multi-media product.
415 User Controls for Captions and Audio Descriptions		
415.1.1 Caption Controls	Not applicable	The product is not a video or multi-media product.
415.1.2 Audio Description Controls	Not applicable	The product is not a video or multi-media product.

Chapter 6 Support Documentation and Services

Criteria	Conformance Level	Remarks and explanations
601.1 Scope		
602 Support Documentation		
602.2 Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide
602.3 Electronic Support Documentation	Supports	Website provides user guide
602.4 Alternate Formats for Non-Electronic Support Documentation	Supports	User guide is provided as an E-book to the customer
603 Support Services		
603.2 Information on Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide
603.3 Accommodation of Communication Needs	Not applicable	Customer support service contact details are available in the user guide and on website. Specific support for persons with disability is not provided

What is the Voluntary Product Accessibility Template (VPAT)?

The purpose of the Voluntary Product Accessibility Template is to assist Federal contracting officials in making preliminary assessments regarding the availability of commercial Electronic and Information Technology products and services with features that support accessibility.

The first table of the Template provides a summary view of the Section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. In the subsequent tables, the first column contains the numbered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

For additional information on these and other accessories, contact your Xerox sales representative or call 1-800-ASK-XEROX (1-800-275-9376).

© 2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR22162

Other company trademarks are also acknowledged.

Document Version: 1.0 (January 2017).

Voluntary Product Accessibility Template® and VPAT® are registered service marks of the Information Technology Industry Council (ITI).

Xerox Accessibility Section 508 Conformance Report

Voluntary Product Accessibility Template® (VPAT®) V2.0

Xerox® AltaLink® C8030/35/45/55/70 MFP



Learn more about Xerox and Section 508 at our website:

www.xerox.com/Section508

Summary Table – Voluntary Product Accessibility Template® (VPAT®)

Criteria	Conformance Level	Remarks and explanations
Chapter 3: Functional Performance Criteria	Supports	The product is compliant with Chapter 3
Chapter 4: Hardware	Supports with exceptions	Compliant with minor exceptions concerning speech, braille, and input controls
Chapter 5: Software	Not applicable	The product does not support the software criteria set forth
Chapter 6: Support Documentation and Services	Supports	The centralization of documentation, training, and support services for most Xerox products allows us to achieve compliance across the corporation.

Software Version Evaluated: 101.001.008

Accessories Included in Evaluation: external keyboard, narrator (inbuilt in windows), headset, and XCA

Evaluation Methods Used: testing based on general product knowledge, similar to another evaluated product, and testing with assistive technologies

Chapter 3: Functional Performance Criteria (FPC)

Criteria	Conformance Level	Remarks and explanations
302.1 Without Vision	Supports	Person without vision can make use of the rocker switch behind the door to power on/off the machine. Also, supported with XCA as the speech output can be directed to the individuals
302.2 With Limited Vision	Supports	Person with limited vision is able to perform all the operations available based on limited vision of 20/70
302.3 Without Perception of Color	Supports	At least one mode of operation that does not require user perception of color is available
302.4 Without Hearing	Supports	One mode of operation that does not require user hearing is available
302.5 With Limited Hearing	Supports	One mode of operation that does not require user limited hearing is available
302.6 Without Speech	Not applicable	Speech is not required for this product
302.7 With Limited Manipulation	Supports	At least one mode of operation that does not require fine motor control or simultaneous manual operations is available
302.8 With Limited Reach and Strength	Supports	At least one mode of operation that does not require limited reach and limited strength is available
302.9 With limited Language, Cognitive, and Learning Abilities	Supports	Features are provided for individuals with limited cognitive, language, and learning abilities for simpler and easier use

Chapter 4: Hardware

Criteria	Conformance Level	Remarks and explanations
402 Closed Functionality		
402.1 General		
402.2 Speech-Output Enabled		
402.2.1 Information Displayed On-Screen	Supports	Speech is enabled via XCA. However machine cannot be powered on/off via XCA.
402.2.2 Transactional Outputs	Not applicable	There is no transactional output
402.2.3 Speech Delivery Type and Coordination	Supports	Speech is enabled via XCA and can be directed to individuals via headsets. However, machine cannot be powered on/off via XCA
402.2.4 User Control	Supports with exceptions	Speech is enabled via XCA. However, there is no repeat and pause option
402.2.5 Braille Instructions	Supports with exceptions	Speech output is not supported in the machine but is via XCA. XCA is specifically set up to enable speech. Using XCA it is assumed the user is aware of the accessibility features
402.3 Volume		
402.3.1 Private Listening	Supports	This product provides a mode of operation for controlling the volume when in private listening mode
402.3.2 Non-private Listening	Supports with exceptions	On / Off is not a feature of XCA. On/Off operations are

Criteria	Conformance Level	Remarks and explanations
		done in hardware but the device does not provide speech output Speech is enabled via XCA. However, there are no volume controls in XCA."
402.4 Characters on Display Screens	Supports	At least one mode of characters displayed on the screen is in sans serif font is available
402.5 Characters on Variable Message Signs	Not applicable	This product does not have variable message signs
403 Biometrics		
403.1 General	Not applicable	Biometric forms are not used.
404 Preservation of Information Provided for Accessibility		
404.1 General	Not applicable	The device does not transmit or conduct information or communication.
405 Privacy		
405.1 General	Supports	The same degree of privacy of input and output is provided to all individuals
406 Standard Connections		
406.1 General	Supports	The data connections are fax line and internet cable and they are industry standard formats
407 Operable Parts		
407.2 Contrast	Supports	The product provides keys and controls with contrast visually from background surfaces
407.3 Input Controls		
407.3.1 Tactilely Discernible	Supports	Input controls are operable by touch and tactilely discernible without activation.
407.3.2 Alphabetic Keys	Supports with exceptions	Through external keyboard, user can enter the text for providing the email destination of the job but user will not be able to go to that 'editable text' field in LUI via keyboard
407.3.3 Numeric Keys	Supports with exceptions	Through external keyboard, user can enter the numeric values for providing the quantity of the job but user will not be able to go to that 'quantity' field in LUI via keyboard
407.4 Key Repeat	Not applicable	Key repeat is not supported.
407.5 Timed Response	Supports with exceptions	Alert provided only visually but not by sound
407.6 Operation	Supports	Controls do not require simultaneous use of two hands, and the force to activate hand-operated controls is less than 5 lbs.
407.7 Tickets, Fare Cards, and Keycards	Not applicable	Tickets, Fare card or keycard is not used in product
407.8 Reach Height and Depth		

Criteria	Conformance Level	Remarks and explanations
407.8.1 Vertical Reference Plane	Supports	At least one of each type of operable part of stationary ICT at a height conforming to 407.8.2 or 407.8.3 is available
407.8.1.1 Vertical Plane for Side Reach	Supports	Where a side reach is provided, the vertical reference plane is 48 inches (1220 mm) long minimum.
407.8.1.2 Vertical Plane for Forward Reach.	Supports	Where a forward reach is provided, the vertical reference plane is 30 inches (760 mm) long minimum
407.8.2 Side Reach	Supports	Where a side reach requires a reach over a portion of the ICT, the height of that portion of the ICT is 34 inches (865 mm) maximum.
407.8.2.1 Unobstructed Side Reach	Supports	Where the operable part is located 10 inches (255 mm) or less beyond the vertical reference plane, the operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor.
407.8.2.2 Obstructed Side Reach	Supports	All operable controls are within specification.
407.8.3 Forward Reach	Supports	Where a forward reach allows a reach over a portion of the ICT, the height of that portion of the ICT shall be 34 inches (865 mm) maximum
407.8.3.1 Unobstructed Forward Reach	Supports	The operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor
407.8.3.2 Obstructed Forward Reach	Supports	Supports maximum allowable forward reach to an operable part is 25inches
407.8.3.2.1 Operable Part Height for ICT with Obstructed Forward Reach	Supports	All operable parts are within specification
407.8.3.2.2 Knee and Toe Space under ICT with Obstructed Forward Reach	Not applicable	There are no operable controls.
408 Display Screens		
408.2 Visibility	Supports	At least one display screen is visible from a point located 40inches above floor space
408.3 Flashing	Supports	The power key LED conforms
409 Status Indicators		
409.1 General	Supports	Rocker switch provides visual and tactile feedback
410 Color Coding		
410.1 General	Supports	Color coding and additional means of unique identification (e.g., text and symbols) are used.
411 Audible Signals		
411.1 General	Supports	Audible signals and additional means of unique identification (e.g., cues) are used.
412 ICT with Two-Way Voice Communication		
412.2 Volume Gain		
412.2.1 Volume Gain for Wireline Telephones	Not applicable	This product does not use analog or digital wireline telephones.
412.2.2 Volume Gain for Non-	Not applicable	The device does not support bi-directional voice

Criteria	Conformance Level	Remarks and explanations
Wireline ICT		communication over a telephone line.
412.3 Interference Reductions and Magnetic Coupling		
412.3.1 Wireless Handsets	Not applicable	The product does not produce electromagnetic fields.
412.3.2 Wireline Handsets	Not applicable	The product does not produce electromagnetic fields.
412.4 Digital Encoding of Speech	Not applicable	This product does not support digital encoding of speech
412.5 Real-time Text Functionality	Not applicable	This product does not support real-time text functionality
412.6 Called ID	Not applicable	Caller ID and/or similar telecommunications are not present.
412.7 Video Communication	Not applicable	The product is not a video or multi-media product.
413 Closed Caption Processing Technologies		
413.1.1 Decoding and Display of Closed Captions	Not applicable	The product is not a video or multi-media product.
413.1.2 Pass-Through of Closed Caption Data	Not applicable	The device does not transmit or conduct information or communication.
414 Audio Description Processing Technologies		
414.1.1 Digital Television Tuners	Not applicable	The product is not a video or multi-media product.
414.1.2 Other ICT	Not applicable	The product is not a video or multi-media product.
415 User Controls for Captions and Audio Descriptions		
415.1.1 Caption Controls	Not applicable	The product is not a video or multi-media product.
415.1.2 Audio Description Controls	Not applicable	The product is not a video or multi-media product.

Chapter 6 Support Documentation and Services

Criteria	Conformance Level	Remarks and explanations
601.1 Scope		
602 Support Documentation		
602.2 Accessibility and Compatibility Features	Supports	Accessibility and compatibility information is available on www.xerox.com/section508/ .
602.3 Electronic Support Documentation	Supports	Website provides guide to the device
602.4 Alternate Formats for Non-Electronic Support Documentation	Supports	User guide is provided as an E-book to the customer
603 Support Services		
603.2 Information on Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide

Criteria	Conformance Level	Remarks and explanations
603.3 Accommodation of Communication Needs	Not applicable	Customer support service contact details available in the user guide and also available on website. Specific support for persons with disability not provided.

What is the Voluntary Product Accessibility Template (VPAT)?

The purpose of the Voluntary Product Accessibility Template is to assist Federal contracting officials in making preliminary assessments regarding the availability of commercial Electronic and Information Technology products and services with features that support accessibility.

The first table of the Template provides a summary view of the Section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. In the subsequent tables, the first column contains the numbered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

For additional information on these and other accessories, contact your Xerox sales representative or call 1-800-ASK-XEROX (1-800-275-9376).

© 2017 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR22162
Other company trademarks are also acknowledged.
Document Version: 1.0 (January 2017).

Voluntary Product Accessibility Template® and VPAT® are registered service marks of the Information Technology Industry Council (ITI).

Xerox Accessibility Section 508 Conformance Report

Voluntary Product Accessibility Template® (VPAT®) V2.0

Xerox® AltaLink® B8045/55/65/75/90 MFP



Learn more about Xerox and Section 508 at our website:

www.xerox.com/Section508

Summary Table – Voluntary Product Accessibility Template® (VPAT®)

Criteria	Conformance Level	Remarks and explanations
Chapter 3: Functional Performance Criteria	Supports	The product is compliant with Chapter 3.
Chapter 4: Hardware	Supports with exceptions	Compliant with minor exceptions concerning speech, volume, status indicators, and input controls
Chapter 5: Software	Not applicable	The product does not support the software criteria set forth
Chapter 6: Support Documentation and Services	Supports	The centralization of documentation, training, and support services for most Xerox products allows us to achieve compliance across the corporation.

Software Version Evaluated: device SW version 101.008.008.12230

Accessories Included in Evaluation: external keyboard, narrator (inbuilt in Windows), headset, and XCA

Evaluation Methods Used: testing based on general product knowledge, similar to another evaluated product, and testing with assistive technologies

Chapter 3: Functional Performance Criteria (FPC)

Criteria	Conformance Level	Remarks and explanations
302.1 Without Vision	Supports	At least one mode of operation that does not require user vision is available
302.2 With Limited Vision	Supports	At least one mode of operation that enables users to make use of limited vision is available
302.3 Without Perception of Color	Supports	At least one mode of operation that does not require user perception of color is available
302.4 Without Hearing	Supports	One mode of operation that does not require user hearing is available
302.5 With Limited Hearing	Supports	One mode of operation that does not require user limited hearing is available
302.6 Without Speech	Not applicable	Speech is not required for this product
302.7 With Limited Manipulation	Supports	At least one mode of operation that does not require fine motor control or simultaneous manual operations is available
302.8 With Limited Reach and Strength	Supports	At least one mode of operation that does not require limited reach and limited strength is available
302.9 With limited Language, Cognitive, and Learning Abilities	Supports	Features are provided for individuals with limited cognitive, language, and learning abilities for simpler and easier use

Chapter 4: Hardware

Criteria	Conformance Level	Remarks and explanations
402 Closed Functionality		
402.1 General		
402.2 Speech-Output Enabled		
402.2.1 Information Displayed On-Screen	Supports	Speech is enabled via XCA. However, machine cannot be powered on/off via XCA.
402.2.2 Transactional Outputs	Not applicable	There is no transactional output
402.2.3 Speech Delivery Type and Coordination	Supports	Speech output is delivered through an industry standard connector or a telephone headset. Output is coordinated with information displayed on the screen.
402.2.4 User Control	Supports with exceptions	Speech is enabled via XCA. However, there is no repeat and pause option.
402.2.5 Braille Instructions	Supports with exceptions	Speech output is not supported in the machine but is via XCA and XCA is specifically set up to enable speech, i.e. in using XCA it is assumed the user is aware of the accessibility features
402.3 Volume		
402.3.1 Private Listening	Supports	Speech is enabled via XCA and can be directed to

Criteria	Conformance Level	Remarks and explanations
		individuals via headsets. On/off is not a feature of XCA. On/off functionality supported via rocker switch behind door
402.3.2 Non-private Listening	Supports with exceptions	Speech is enabled via XCA. However machine cannot be powered on/off via XCA and there are no volume controls in XCA
402.4 Characters on Display Screens	Supports with exceptions	All text is sans serif but text is 4mm
402.5 Characters on Variable Message Signs	Not applicable	This product does not have variable message signs
403 Biometrics		
403.1 General	Not applicable	Biometric forms are not used.
404 Preservation of Information Provided for Accessibility		
404.1 General	Not applicable	The device does not transmit or conduct information or communication.
405 Privacy		
405.1 General	Supports	The same degree of privacy of input and output is provided to all individuals
406 Standard Connections		
406.1 General	Supports	At least one type of connection conform to industry standard non-priority format.
407 Operable Parts		
407.2 Contrast	Supports	The product provides keys and controls with contrast visually from background surfaces
407.3 Input Controls		
407.3.1 Tactilely Discernible	Supports	Input controls are operable by touch and tactilely discernible without activation.
407.3.2 Alphabetic Keys	Supports with exceptions	Through external keyboard, user can enter the text for providing the email destination of the job. User will not be able to go to that 'editable text' field in LUI via keyboard
407.3.3 Numeric Keys	Supports with exceptions	Through external keyboard, user can enter the numeric values for providing the quantity of the job. User will not be able to go to that 'quantity' field in LUI via keyboard
407.4 Key Repeat	Not applicable	Key repeat is not supported.
407.5 Timed Response	Supports with exceptions	Alert provided only visually but not by sound
407.6 Operation	Supports	Controls do not require simultaneous use of two hands, and the force to activate hand-operated controls is less than 5 lbs.
407.7 Tickets, Fare Cards, and Keycards	Not applicable	Tickets, Fare card or keycard is not used in product
407.8 Reach Height and Depth		

Criteria	Conformance Level	Remarks and explanations
407.8.1 Vertical Reference Plane	Supports	At least one of each type of operable part of stationary ICT at a height conforming to 407.8.2 or 407.8.3 is available
407.8.1.1 Vertical Plane for Side Reach	Supports	Where a side reach is provided, the vertical reference plane is 48 inches (1220 mm) long minimum.
407.8.1.2 Vertical Plane for Forward Reach.	Supports	(1) Where a forward reach is provided, the vertical reference plane is 30 inches (760 mm) long minimum
407.8.2 Side Reach	Supports	Where a side reach requires a reach over a portion of the ICT, the height of that portion of the ICT is 34 inches (865 mm) maximum.
407.8.2.1 Unobstructed Side Reach	Supports	Where the operable part is located 10 inches (255 mm) or less beyond the vertical reference plane, the operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor.
407.8.2.2 Obstructed Side Reach	Supports	All operable controls are within specification.
407.8.3 Forward Reach	Supports	Where a forward reach allows a reach over a portion of the ICT, the height of that portion of the ICT shall be 34 inches (865 mm) maximum
407.8.3.1 Unobstructed Forward Reach	Supports	The operable part is 48 inches (1220 mm) high maximum and 15 inches (380 mm) high minimum above the floor
407.8.3.2 Obstructed Forward Reach	Supports	Supports maximum allowable forward reach to an operable part is 25inches
407.8.3.2.1 Operable Part Height for ICT with Obstructed Forward Reach	Supports	All operable parts are within specification
407.8.3.2.2 Knee and Toe Space under ICT with Obstructed Forward Reach	Not applicable	There are no operable controls.
408 Display Screens		
408.2 Visibility	Supports	At least one display screen is visible from a point located 40inches above floor space
408.3 Flashing	Supports	The power key LED conforms
409 Status Indicators		
409.1 General	Supports with exceptions	After inserting the document in DADH, the Status is indicated visually by LED light. However it doesn't provide any sound to indicate the status.
410 Color Coding		
410.1 General	Supports	Color coding and additional means of unique identification (e.g., text and symbols) are used.
411 Audible Signals		
411.1 General	Supports	Audible signals and additional means of unique identification (e.g., cues) are used.
412 ICT with Two-Way Voice Communication		
412.2 Volume Gain		
412.2.1 Volume Gain for Wireline	Not applicable	This product does not use analog or digital wireline

Criteria	Conformance Level	Remarks and explanations
Telephones		telephones.
412.2.2 Volume Gain for Non-Wireline ICT	Not applicable	The device does not support bi-directional voice communication over a telephone line.
412.3 Interference Reductions and Magnetic Coupling		
412.3.1 Wireless Handsets	Not applicable	The product does not produce electromagnetic fields.
412.3.2 Wireline Handsets	Not applicable	The product does not produce electromagnetic fields.
412.4 Digital Encoding of Speech	Not applicable	This product does not support digital encoding of speech
412.5 Real-time Text Functionality	Not applicable	This product does not support real-time functionality
412.6 Called ID	Not applicable	Caller ID and/or similar telecommunications are not present.
412.7 Video Communication	Not applicable	The product is not a video or multi-media product.
413 Closed Caption Processing Technologies		
413.1.1 Decoding and Display of Closed Captions	Not applicable	The product is not a video or multi-media product.
413.1.2 Pass-Through of Closed Caption Data	Not applicable	The device does not transmit or conduct information or communication.
414 Audio Description Processing Technologies		
414.1.1 Digital Television Tuners	Not applicable	The product is not a video or multi-media product.
414.1.2 Other ICT	Not applicable	The product is not a video or multi-media product.
415 User Controls for Captions and Audio Descriptions		
415.1.1 Caption Controls	Not applicable	The product is not a video or multi-media product.
415.1.2 Audio Description Controls	Not applicable	The product is not a video or multi-media product.

Chapter 6 Support Documentation and Services

Criteria	Conformance Level	Remarks and explanations
601.1 Scope		
602 Support Documentation		
602.2 Accessibility and Compatibility Features	Supports	XCA is provided to the customer with the user guide
602.3 Electronic Support Documentation	Supports	Website provides user guide
602.4 Alternate Formats for Non-Electronic Support Documentation	Supports	User guide is provided as an E-book to the customer
603 Support Services		
603.2 Information on	Supports	XCA is provided to the customer with the user guide

Criteria	Conformance Level	Remarks and explanations
Accessibility and Compatibility Features		
603.3 Accommodation of Communication Needs	Not applicable	Customer support service contact details are available in the user guide and also on website. Specific support for persons with disability is not provided

What is the Voluntary Product Accessibility Template (VPAT)?

The purpose of the Voluntary Product Accessibility Template is to assist Federal contracting officials in making preliminary assessments regarding the availability of commercial Electronic and Information Technology products and services with features that support accessibility.

The first table of the Template provides a summary view of the Section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. In the subsequent tables, the first column contains the numbered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

For additional information on these and other accessories, contact your Xerox sales representative or call 1-800-ASK-XEROX (1-800-275-9376).

© 2017 Xerox Corporation. All rights reserved. Xerox®, AltaLink®, and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR22162

Other company trademarks are also acknowledged.

Document Version: 1.0 (January 2017).

Voluntary Product Accessibility Template® and VPAT® are registered service marks of the Information Technology Industry Council (ITI).

The Safety of Xerox® Products

Facts about the safety of Xerox® products.



© 2019 Xerox Corporation. All rights reserved. Xerox® is a trademark of Xerox Corporation in the United States and/or other countries. BR22041

Other company trademarks are also acknowledged.

Document Version: 1.3 (August 2019).

Contents

1. General Information	1
Environment, Health, Safety and Sustainability Policy at Xerox	1
Safety Data Sheets	2
General Safety Practices	2
Equipment Design	2
Consumables	3
2. Xerox® Products	4
Electromagnetic Compatibility	4
Ergonomics/Human Factors.....	4
Document Illumination.....	4
Lasers.....	4
3. Xerox® Supplies	5
Materials Safety Evaluation	5
Toners and Developers.....	5
Liquid Inks	6
Solid Inks.....	6
Fuser Lubricants	6
Photoreceptors	6
4. Indoor Air Quality and Emissions	7
Ozone.....	7
Volatile Organic Compounds (VOCs)	7
Particulates and Dust	8
Odors.....	8
5. Additional Topics	9
Audible Noise	9
Product Service and Maintenance	9
Disposal of Spent Supplies and Equipment.....	9
Service Materials.....	10
Equipment	10
6. Additional Information.....	11

1. General Information

Environment, Health, Safety and Sustainability Policy at Xerox

The Environment, Health, Safety, and Sustainability (EHS&S) organization at Xerox ensures company-wide adherence to Xerox's environment, health, safety, and sustainability policy. The governance model we use to accomplish this includes clearly defined goals, a single set of worldwide standards, and an audit process that ensures conformance to these requirements. Our EHS&S governance and policy, adopted in 1991, forms the foundation of our environmental leadership program.

It is the policy of Xerox Corporation to:

- Comply with applicable environment, health and safety laws, rules, regulations and Xerox Standards;
- Take appropriate measures to protect the environment and health and safety of our employees, customers, suppliers and neighbors from unacceptable risk;
- Take appropriate measures to prevent workplace injuries and illnesses; provide employees with a safe and healthy work environment;
- Assess environment, health, and safety impacts before starting a new activity or project;
- Comprehend environment, health, and safety impacts in the design and acquisition of products and services;
- Eliminate unacceptable risks from facilities, products, services and processes;
- Strive for continual improvement of its environmental management system and to conserve natural resources, eliminate the use of toxic and hazardous materials; prevent pollution; recover, reuse, recycle;
- Address climate change by reducing the carbon footprint of our operations, products and services; and
- Require suppliers to adhere to applicable environment, health, and safety laws, rules, regulations and Xerox Standards.

Overview

To ensure full compliance with the above policy, health, safety and environmental considerations are an essential element of the product and materials design and review process, involving internal and external world-class experts.

Extensive system testing is conducted under a variety of simulated field and stress conditions to verify that all the health and safety requirements have been met. Our internal test groups conduct some of these tests while external testing organizations perform others.

Xerox has a long history of proactively assessing the health and safety of the materials used in its products using a wide variety of methods. These measures drive elimination of the use of persistent, bio-accumulative and toxic materials throughout the supply chain and the safety of our equipment and consumable products.

Whenever new information raises a concern about the safety of a product, we investigate and, when warranted, take prompt action with health and safety consideration being our highest priority.

Safety Data Sheets

Xerox prepares two types of data sheets that summarize safety and health information for our equipment and consumables products:

- **Product Safety Data Sheets** (PSDS) contain information about the mechanical, electrical and environmental attributes of our equipment as well as product emission data.
- **Safety Data Sheets** (SDS) provide information on the globally recognized classification and the safe use of products that may be chemical substances or mixtures. They also contain storage, shipping and disposal information.

General Safety Practices

To ensure the safety of those who use and care for our equipment, it is important to observe these fundamental rules:

- Site the equipment according to published Xerox® installation requirements. When moving equipment to a new location, review installation requirements.
- Connect the equipment to a properly grounded electrical service outlet.
- Comply with all caution and warning labels in order to avoid potentially hazardous conditions.
- Do not bypass or defeat interlocked covers. These covers prevent creation of hazardous conditions, which could occur if they were opened.
- Only trained service personnel may remove covers or guards held in place by fasteners that cannot be detached without using tools.
- Only use Xerox approved maintenance procedures and materials.
- Stop the equipment immediately, disconnect it from its power supply and have it serviced before the next use in the event of unusual noises, odors or smoke.
- Dispose of spent materials and products according to information provided on Safety Data Sheets, which can be found on www.xerox.com/environment
- Do not stare at equipment light sources, which can produce temporary nuisance effects or discomfort.

Equipment Design

Xerox policy requires that products meet safety standards that are at least as strict as the generally accepted standards of approval agencies and government regulations. For each product brought to market, Xerox has a comprehensive Product Safety Requirement List that details the specific safety requirements.

All possible hazards are assessed: electrical, mechanical, chemical, biological, radiation, heat, emissions and noise. Results of assessments must be satisfactory in all areas before shipping equipment to the customer.

In addition to these assessments, service procedures, service materials, special tools and the operator's manual must all be approved prior to customer shipments. Installation instructions define minimum product space requirements to ensure proper equipment performance and to provide adequate access for service.

Xerox® products are typically submitted to a nationally recognized testing laboratory such as Underwriters Laboratories® (UL), Canadian Standards Association (CSA) or TUV Rheinland®, resulting in product certification to the latest country-specific version of internationally accepted product safety standards, such as IEC 60950 (Safety of Information Technology Equipment).

Products are also CB Scheme Certified, and CE marked for sales in European Union markets and the equivalent schemes of other countries where they may be marketed.

Consumables

Xerox takes a conservative position on potential health risks to our employees and customers. Accordingly, Xerox has established strict internal standards limiting the use of potentially hazardous materials in consumable products. In some cases, this includes setting internal company exposure limits, known as Xerox Exposure Limits (XEL), for specific chemical or physical agents. Xerox Exposure Limits are more stringent than external consensus or regulatory limits.

2. Xerox® Products

Electromagnetic Compatibility

Xerox® products are designed to function properly in the intended electromagnetic environment without causing harmful interference to nearby equipment or radio communication services. In this regard, Xerox® products comply with all governmental regulations covering Electromagnetic Compatibility (EMC). Appropriate product testing verifies compliance.

Ergonomics/Human Factors

Human factors are an integral part of our design process. Our multidisciplinary team of professionals evaluates Xerox® products to ensure usability by our customers, serviceability by our technicians and ease of assembly by our manufacturing personnel.

Document Illumination

Staring at lamps can sometimes produce an afterimage, but this is of short duration and has no permanent effects. Due to the intensity of some light sources, some lamp systems are interlocked with the platen cover to prevent this. We recommend that all platens be covered while making copies, to minimize exposure and facilitate good copy quality.

Lasers

Xerox® products containing lasers present no hazard to equipment operators or bystanders and are designed and built to comply with the strict safety requirements of governmental and international standards. Product designs ensure that potentially harmful laser beams are contained within the equipment. Covers and shields need not, and should not, be removed for customer maintenance. Covers that may be removed by Xerox service personnel are labeled to indicate potential laser hazards. No service mode requires direct viewing of the laser beam or permits the beam to exit the confines of the equipment. Service personnel following established adjustment procedures are not exposed to potentially harmful laser beams.

3. Xerox® Supplies

Materials Safety Evaluation

Materials used in our consumable products are classified and labeled in compliance with the Globally Harmonized System of Classification and Labeling of Chemicals (GHS) and meet our own stringent internal safety requirements. During the assessment of any material or product, both its inherent properties (potential hazards) and the potential exposures to customers and service personnel are considered.

The various materials used in imaging processes undergo a full toxicological evaluation, which reviews published technical data and information obtained from responsible testing. The safety evaluation process considers possible acute and chronic effects as well as the potential for eye and skin irritation. Various bacterial and mammalian cell type tests are used as predictors of potential genotoxic effects.

When published data is lacking, additional testing may be required. If that is the case, all tests are performed to the Organization for Economic Cooperation and Development (OECD) methods by independent laboratories that operate in accordance with the rules of good laboratory practice, and the results are documented and placed into the health and safety archives. Further, all laboratories used in safety testing are accredited by, or meet the standards of, the American Association for Accreditation of Laboratory Animal Care. Responsible use and humane treatment of animals are basic requirements of sound scientific research and the generation of valid test data. Whenever feasible, we utilize alternatives to animal testing; however, viable alternatives do not always exist. In all instances, we ensure that our safety testing activities are in full compliance with worldwide regulatory standards and requirements.

Results of the toxicological evaluation are in Safety Data Sheets and the details of the review and any applicable test reports are available to appropriate health and safety regulatory agencies when needed.

Toners and Developers

Some Xerox® toners are fine powders composed of plastics, colorants and small quantities of functional additives. They are not considered to be hazardous preparations according to any regulatory classification criteria. Toner constituents must not only produce images having high xerographic quality but also pass our health and safety reviews.

The toners are typically designed using styrene-acrylic, styrene-butadiene or polyester polymers. In black toners, several different specialty grade carbon blacks or iron oxide are used as colorant, while various dyes or pigments are employed for color images. During the toner manufacturing process, the carbon black (or other colorant) and polymer are combined in such a way that the colorant becomes encapsulated by the polymer.

Under normal operating conditions and other foreseeable conditions, the toners are entirely stable, and no significant decomposition occurs. When exposed to the proper combination of heat and pressure, the toner simply flows and adheres to the paper.

Developers are composed of a carrier material and toner. Xerox® carriers are based on special grades of sand, glass, steel or ferrite types of materials. They are generally coated with a small amount of special polymer to achieve the desired functional behavior in the xerographic equipment.

A comprehensive assessment of new materials in our toners is conducted to ensure conformance with applicable global registration, hazard communication and waste handling and disposal requirements. Because of our stringent requirements, Xerox® toners and printing products are non-carcinogenic and non-mutagenic. In addition, these products do not cause adverse developmental or reproductive effects; pose a toxicity hazard to humans or aquatic species; cause a permanent adverse impact to the skin, eyes or respiratory system; or have the potential to generate federally regulated hazardous waste. Xerox was the first in our industry to evaluate the health effects of toner and did so for over 30 years.

Liquid Inks

Most Xerox® liquid inks are aqueous (water based) inks containing dispersing agents and dyes or pigments. Before being placed on the market, each of the inks undergoes a rigorous safety evaluation to ensure all regulatory requirements are met and that the inks meet the strict requirements of Xerox internal standards.

For some specific applications, such as Direct-to-Object printing, UV curable liquid inks are used. These inks, like all other materials, undergo extensive safety evaluation. They are classified according to GHS and labeled appropriately with all potential hazards outlined in the Safety Data Sheets, along with guidelines for safe handling, storage and disposal.

Solid Inks

Xerox uses solid inks in some imaging applications such as plotters and printers. The various solid inks contain polyethylene, waxes, resins, dyes and pigments. The resultant material is a waxy solid block that is transferred to the printed surface under specific heat and pressure specifications. All the materials used in the manufacture of solid inks are subject to the same rigorous safety evaluation as other imaging materials.

Fuser Lubricants

Some xerographic processes use lubricants as release agents during the fusing process. These lubricants are inert, non-hazardous silicone oils and greases, which have high thermal stability. The lubricants are not mineral oils and are not subject to regulatory controls for such materials.

Photoreceptors

A xerographic photoreceptor is a multilayer device in which photo-conducting layers are very tightly bonded to a substrate. The substrate may be a rigid aluminum drum or a flexible metal belt or polyester film. Most current photoreceptors use a proprietary organic photoconductor. Like all imaging materials, photoreceptor constituents are subject to rigorous safety evaluation.

4. Indoor Air Quality and Emissions

We design our products to ensure that they can be safely located in typical office areas near employee workspaces. Under normal operating conditions and with proper maintenance, machines meet or exceed legal requirements and current standards for emissions and are in conformance with select internationally recognized voluntary guidelines. Additional information about the emission characteristics of Xerox® equipment is in the Product Safety Data Sheets.

Xerox supports our customers' responsibility for maintaining excellent indoor air quality in the workplace. Many factors affect the quality of indoor air including ventilation, office furnishings and building materials, in addition to the type of office equipment and use patterns. Xerox® equipment is tested in conformance with rigorous emission testing protocols to ensure that we meet or exceed current standards and acceptable best practices. For example, we set and adhere to strict internal limits on the amount of ozone, volatile organic compounds, and particulate substances emitted from xerographic products.

Ozone

In xerographic devices, small quantities of ozone are produced as a byproduct of the printing process. Ozone is generated only when the machine is copying or printing. Xerox Ozone Management Guidelines require that equipment situated in locations that do not meet either space or temperature and humidity requirements be equipped with a filter to reduce ozone to an acceptable level. Some equipment is equipped with ozone filters at the factory while others may be retrofitted at the placement site. With production printing equipment, the exposure to ozone is controlled by ducting which routes the emissions away from the area. Xerox emission levels of ozone are substantially below internationally recognized exposure limits. The **Facts about Ozone** publication is available upon request or at www.xerox.com/environment

Volatile Organic Compounds (VOCs)

In some conditions, volatile organic compounds may be emitted during and immediately after copying or printing. The concentrations are low, typically less than 1/100th of the occupational exposure limits for such compounds. Volatile compounds are measured in special inert chambers because their levels are less than the levels found in typical room interiors due to building materials, floor covering and furniture. Measured levels, as included on the Product Safety Data Sheets, also meet many global ecolabel requirements.

Particulates and Dust

During a product's operation, very small amounts of paper dust and toner may become airborne. Most dust created inside the machine is drawn through the heat exhausts and trapped by filters.

Dust associated with copying and printing consists primarily of paper particles and fibers. When paper is handled outside the equipment, paper fragments are also generated. Ultimately, levels of paper dust depend on the composition and quality of the paper used.

Less than 10 percent of the dust generated is toner particles. The levels are significantly below the standard exposure limits for respirable dust.

Odors

Xerox makes every effort to ensure that our equipment does not emit objectionable odors into the workplace. However, since some chemicals have very low odor thresholds, some people with a sensitive sense of smell may sometimes detect faint odors, even though the concentration of the chemical is significantly below any that would present a potential health concern.

5. Additional Topics

Audible Noise

Xerox uses state-of-the art instrumentation and noise test facilities to optimize product designs for low noise and enhanced comfort. Xerox® products do not produce noise levels expected to damage human hearing. Noise emission levels meet various ecolabel and ergonomic guidelines and are well below legally mandated exposure limits established around the world.

Product Service and Maintenance

Environmental health and safety personnel at Xerox review and approve all service procedures and materials prior to field usage. They assess and control any potential mechanical, electrical, chemical or physical hazards such as lasers, noise, etc. to minimize exposures of our employees and customers. Field usage of these procedures and materials is monitored, and product retrofits, warning labels or special bulletins are made when appropriate.

Xerox has created ways for customers to service their own equipment using web-based service procedures or described to the customer over the telephone. These service procedures have been reviewed and approved by qualified health and safety personnel to ensure that customers are not significantly exposed to physical hazards, chemical or physical agents, ergonomic stressors, or hazardous electrical energy.

Disposal of Spent Supplies and Equipment

Proper disposal of waste materials minimizes environmental impacts. The environmental management program at Xerox identifies hazardous waste materials for proper disposal and encourages recycling or reclaiming of waste products. All materials used in the various imaging processes are evaluated against the following criteria: environmental toxicity and biodegradability, ignitability, corrosivity and reactivity.

Sections 6 and 13 of the Safety Data Sheets provide guidance for managing spills and disposal. For any questions concerning disposal of Xerox® materials, review Safety Data Sheets and observe all applicable governmental regulations.

The Xerox [Green World Alliance \(www.xerox.com/GWA\)](http://www.xerox.com/GWA) collection and reuse/recycling program, in partnership with our customers, results in millions of cartridges and toner containers returned for reuse or recycling each year.

Exceptions or special considerations may apply in the following circumstances:

- Photoreceptors

The photoreceptors used in our modern equipment have met all the criteria to be classified nonhazardous. Return used or damaged Xerox® photoreceptors containing arsenic and selenium to Xerox Corporation or the supplier for disposition. If not returned to Xerox, follow state and local laws regarding disposal of this material. We recommend disposal in a chemical waste landfill.

- Toner or toner cartridges

Toner or toner cartridges can be recycled locally or returned to Xerox through our Green World Alliance program. Incineration is discouraged, as dust clouds from residual toner may be explosive.

- Developer

Developer also meets all criteria for classification as nonhazardous and therefore may be disposed of with normal office refuse. However, state and local requirements may be more restrictive so consult the appropriate state and local authorities.

Service Materials

Safety Data Sheets are available for each of the service materials sold by Xerox. These materials have also been evaluated against hazardous waste criteria to determine proper disposal. If the waste materials are classified hazardous and small quantity generator exemptions do not apply, applicable governmental regulations must be observed for proper disposition.

For additional questions concerning disposal of Xerox® service materials, please review the Safety Data Sheets and observe all applicable governmental regulations.

Equipment

Xerox operates a worldwide equipment takeback and reuse/recycle program as described at www.xerox.com/environment

6. Additional Information

It is a fundamental principle of Xerox Corporation to ensure that our products are safe and do not in any way represent a concern to our customers or employees.

More information is available on the Xerox Environment, Health, Safety and Sustainability website at www.xerox.com/environment or contact:

North America

Askxerox@xerox.com

1.800.ASK.XEROX (1.800.275.9376)

Europe

EHS-Europe@xerox.com

Recommended Media List

Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090 Multifunction Printer

This Recommended Media List contains Xerox® Paper and Specialty Media that has been extensively tested on the Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090 Multifunction Printer for image quality and performance by Xerox® at the Xerox® Media Technology Center.

The paper and specialty media on this list are approved by Xerox and recommended for use in all configurations of the Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090 Multifunction Printer.

All Xerox® Paper and Specialty Media on this list are digitally optimized, designed and manufactured for optimal performance in Xerox digital printing equipment and carry the Domtar 100% Performance Guarantee. Domtar offers a 100% Performance Guarantee for any Xerox® Paper or Specialty Media that is featured on the Recommended Media List for a specific Xerox printer or digital press. This is your assurance that if you are unhappy with the performance of recommended

Xerox® Paper or Specialty Media, Domtar will either take back the unused product and replace it or refund your money – guaranteed.

Domtar Paper Company, LLC. and Domtar Inc., (collectively referred to as “Domtar”), are the exclusive U.S. and Canadian trademark licensees of Xerox® Paper and Specialty Media. Domtar’s and Xerox’s extensive collaborative testing and stringent specifications ensure that we are able to guarantee the performance and consistency of Xerox® Paper and Specialty Media.

Recommended Media List

General Information

Customers should validate that the Best Practices for Operation for the selected Xerox® Paper or Specialty Media are acceptable for their application. When purchasing a particular media product for the first time, customers are advised to purchase small quantities to ensure that expectations are met.

Media observations made in this publication are based on tests conducted using standard images with moderate to heavy image area coverage. Test machines are maintained within specifications defined by user documentation. Where applicable, suggested adjustments and best practices are included to optimize media performance. Note that “size” designation is for sheet dimensions only, and is not used to indicate grain direction.

The Stock Library Montage application can be updated with the most current Recommended Media List by downloading the “Recommended Media List.rml” file from Xerox.com. This file can be found on Xerox.com under the Support and Drivers tab, searching on Altalink. Instructions on how to update the Stock Library Manager media list are included with the file.

To view the most current Recommended Media List, please visit www.xeroxpaperusa.com/resources/recommended-media-list.

Warranty Disclaimer

Domtar and Xerox make no guarantees or warranties, either expressed or implied, concerning the performance, use or replacement of non-Xerox branded media or throughput products. Customers should inquire directly of their paper distributor or manufacturer for any guarantees they may offer. When purchasing a particular media product for the first time, customers are advised to purchase small quantities to insure their expectations are met. The quality of Xerox supplies is consistent from ream to ream and is backed by a 100% guarantee such that if you are unhappy with the performance of recommended Xerox® Paper or Specialty Media, Domtar will either take back the unused product and replace it or refund your money. The quality of non-Xerox branded paper may vary from ream to ream or carton to carton, so for optimum performance on Xerox color equipment, use only the best: Xerox supplies.

To learn more about Xerox® Paper and Specialty Media, please call 1-866-814-2401.

To learn more about the benefits of using Xerox Supplies (toner and ink), please contact your Xerox Supplies Representative at 1.800.822.2200 (U.S.) or 1.800.668.0199 (Canada).

Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090 Multifunction Printer

Item Number	Paper & Specialty Media Description	Size	Paper Type Setting	Weight (gsm)	Trays						Trays						Finisher Capabilities					
					Trays			MSI (Bypass)	PFM	Office Finisher (2KLCSS)	Office Finisher (2KLCSS)			HVF/HV/LVF Booklet Maker Finisher			CZ Folder					
					1	2	3				4	5	6	Stack	Staple	Books (SEF)	Bi-fold (SEF)	Letter 'Z'	Letter 'C'	Additional Information		
Xerox® Vitality® Multipurpose Printer Paper																						
3R02047	20 lb. Bond	8.5 x 11	Bond	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11415	20 lb., Xpress Pack Bond	8.5 x 11	Bond	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R02641	20 lb. HolePunched	8.5 x 11 3HP	HolePunched	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R02051	20 lb. Bond	8.5 x 14	Bond	75	A	A	A	A	A	n	♦	♦	♦	♦	♦	♦	♦	n	n			
3R03761	20 lb. Bond	11 x 17	Bond	75	A	A	A	A	A	n	♦	♦	♦	♦	♦	♦	♦	n	n			
3R02531	24 lb. Bond	8.5 x 11	Bond	90	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11414	24 lb. Bond	8.5 x 11	Bond	90	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R03317	24 lb. HolePunched	8.5 x 11	HolePunched	90	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R03871	24 lb. Bond	11 x 17	Bond	90	A	A	A	A	A	n	♦	♦	♦	♦	♦	♦	♦	n	n			
Xerox® Vitality® Multipurpose Printer Paper, 30% Recycled																						
3R06296	20 lb. Recycled	8.5 x 11	Recycled	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R06297	20 lb. Recycled	8.5 x 11 3HP	Recycled	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R06298	20 lb. Recycled	8.5 x 14	Recycled	75	A	A	A	A	A	n	♦	♦	♦	♦	♦	♦	♦	n	n			
3R06299	20 lb. Recycled	11 x 17	Recycled	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
Xerox® Vitality® Index Paper																						
3R11747	90 lb. Index	8.5 x 11	Lightweight Cardstock	163	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11748	90 lb. Index	17 x 11	Cardstock	163	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11749	110 lb. Index	8.5 x 11	Cardstock	199	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
Xerox® Vitality® Pasetl Multipurpose Printer Paper																						
3R11050	20 lb. Blue	8.5 x 11	Colored	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11051	20 lb. Green	8.5 x 11	Colored	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11052	20 lb. Pink	8.5 x 11	Colored	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11053	20 lb. Yellow	8.5 x 11	Colored	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11055	20 lb. Goldenrod	8.5 x 11	Colored	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			
3R11056	20 lb. Ivory	8.5 x 11	Colored	75	A	A	A	A	A	A	♦	♦	♦	♦	♦	♦	♦	♦	♦			

Notes:
 The Recommended Media List contains Xerox® Paper and Specialty Media, digitally optimized, designed from stringent specifications and manufactured for optimal and constant image quality performance. Xerox® Paper and Specialty Media have undergone rigorous testing by Xerox®.
 Any paper and print media that is featured on the Recommended Media List for a specific Xerox® printer or digital press will give optimum performance. Relative humidity greater than 40% could cause multifeeds.
 The Office Finisher (2KLCSS) is capable of stapling at maximum; (maximum number will decrease if paper weight is greater than 20lb / 75 gsm):
 • 50 Sheets of Letter (8.5 x 11") in Long Edge Feed (LEF) or Short Edge Feed (SEF)
 • 50 Sheets of Tabloid/Ledger (11 x 17"), Legal (8.5 x 14)
 The Office Finisher with Booklet Maker (LVF) is capable of stapling at maximum; (maximum number will decrease if paper weight is greater than 20lb / 75 gsm):
 • 50 Sheets of Letter (8.5 x 11") in Long Edge Feed (LEF) or Short Edge Feed (SEF)
 • 50 Sheets of Tabloid/Ledger (11 x 17") or Legal (8.5 x 14)
 • 15 Sheets, maximum 24lb / 90 gsm, Short Edge Feed (SEF) of Letter (8.5 x 11"), Tabloid/Ledger (11 x 17"), or Legal (8.5 x 14) for the Booklet Maker
 Letter 'Z' and 'C' folding available only when sheets are fed SEF. Max Tray capacity for 'Z' fold is 30 sheets and for Letter 'Z' and 'C' is 40 sheets.



Domtar is the exclusive trademark licensee of the Xerox® Paper and Specialty Media Line within the United States and Canada.

Working collaboratively with the Xerox Corporation and our Media Partners, Domtar designs and manufactures the Xerox® Paper and Specialty Media Line to bring you the most extensive line of digitally optimized products in the United States and Canada.

With the Domtar Performance Guarantee, you can be assured that if you are unhappy with the performance of the product, you may return the unused portion and Domtar will either replace it, or refund your money.

Xerox® Paper and Specialty Media products are distributed by Domtar and are widely available for purchase through office supply dealers, paper merchants, office supply stores, online as well as in selected retail stores.

www.domtar.com

www.xeroxpaperUSA.com | www.xeroxpaper.ca



Xerox® Adaptable Accessibility Solution

Empowering the blind, visually impaired
and people of all abilities.

To keep your business strong, your employees need to feel empowered to perform their best. The Xerox® Adaptable Accessibility Solution makes that happen. It operates on a standard tablet to leverage users' existing working knowledge of technology tools. Plus, audio talk-back provides work independence for key features like Copy, Scan to Email and Faxing—helping minimize the barriers technology can have for people with disabilities.

Technology created for users of all abilities.

Ensures Legislation Compliance and Security

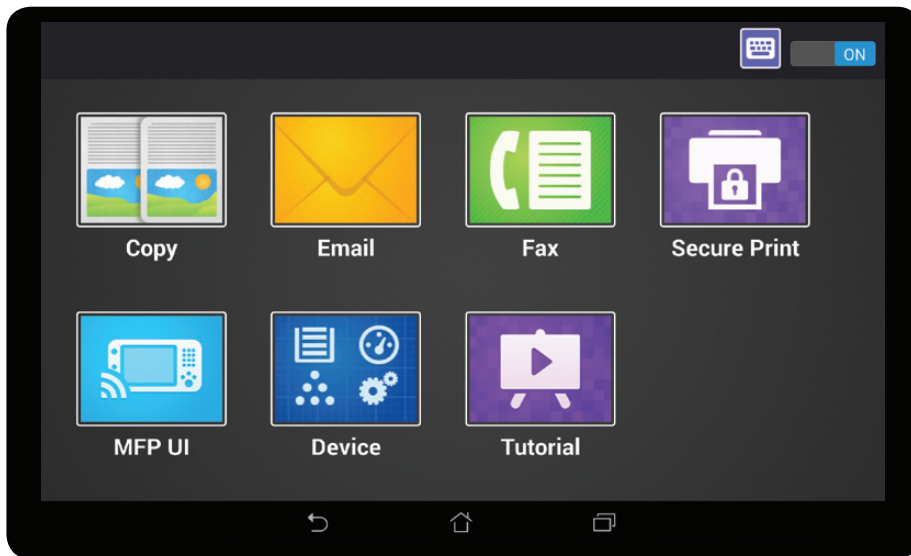
This solution is compliant with the U.S. legislation of the federal Workforce Investment Act of 1998 and amended Section 508 of the Rehabilitation Act. It's integrated with secure solutions like Xerox® Common Access Card authentication for advanced levels of security for sensitive government information. Plus, with Xerox® Secure Print, a unique Pin ID is required for print submission—further enhancing security.

Enhances Workplace Independence

The touch screen of the standard tablet features oversized, easy-to-view application icons for the multifunction features. Combine that with the adjustable mounting bracket that allows them to modify the tablet to their own proper viewing angle—a great flexibility for the visually impaired as well as for those who use wheelchairs. Plus, the USB keyboard provides an easier alternative for data entry for users who prefer this method to navigate through menus and populate fields.

Strengthens Employee Confidence

There are two user modes. User mode one enables audible and talk-back features. That way, blind and visually impaired employees can copy, scan to email and scan with ease. Stress-free accurate task selections can be heard as they are touched on the screen. User mode two displays all features of the multifunction printer user interface. This viewing mode accommodates others using all the solutions and capabilities of the device.



These key multifunction printer features are available with talk-back audio:

- Copy
- Scan to Email
- Fax
- Secure Print Release

Industry-standard tablet

Tutorial available in audio format

Large application icons and touch screen

Robust workflows

- Scan to Email is simple with a local address book on the tablet and USB keyboard.
- Users can scan documents to be turned into searchable PDFs which can be emailed and used with existing technologies providing audible playback.

Of the 15 million visually impaired residents of the United States, nearly 38 percent* are employed. Do you have the resources and tools in place to help them succeed?



Scan this QR code to see how this solution empowers employees at the Association for the Blind and Visually Impaired.

To learn more about the Xerox® Adaptable Accessibility Solution, call your local Xerox sales representative.

*Online Resource for U.S. Disability Statistics. Cornell University. 2013.
©2015 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design®, ConnectKey® and WorkCentre® are trademarks of Xerox Corporation in the United States and/or other countries. BR13804



Touchless Workplace Technologies



Touchless Workplace Technologies

Minimize physical interaction and stay productive with apps for desktop or mobile devices



Workplace Mobile App

Print and scan documents from your mobile devices



Xerox Audio Documents Mobile App

Upload and transform documents into audio files from your tablet or phone



Easy Translator Mobile App and Portal

Translate documents in to 50 different languages instantly



Xerox Proofreader Online Portal

Upload documents and check for plagiarism, grammar, spelling and style using an online portal



Xerox Mobile Link App

Seamlessly connect your Xerox multifunction printer with your mobile device. Open, manipulate, share, and delete scanned or captured documents. Then print, scan or fax with a touch of your mobile device.

Xerox Scan Compression Technology

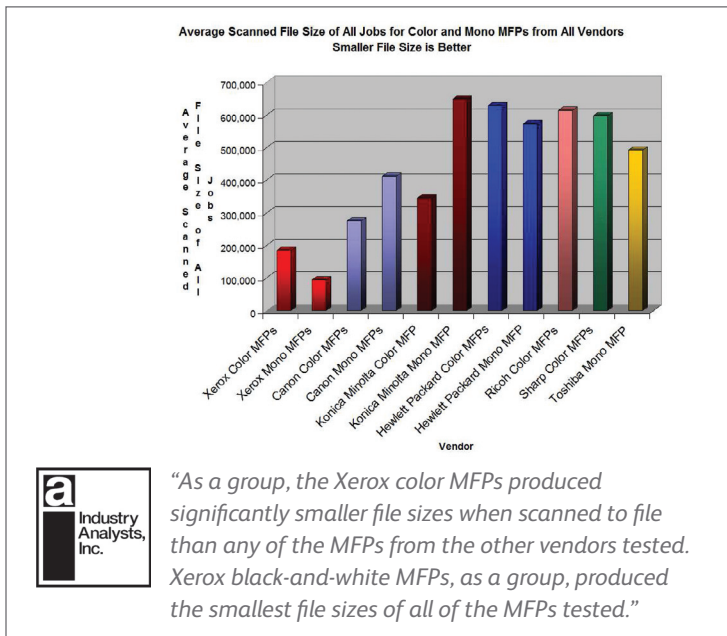
Smaller scan files mean greater office productivity

The power of scanning gives your office more workflow options, making it easy to turn hard copy documents into electronic files for fast distributing, organizing and archiving.

But many popular multifunction devices lack the ability to adequately compress a scanned image, resulting in greater strain on network bandwidth or files with degraded image quality.

Xerox MFPs, however, feature advanced scan-file compression technology that greatly reduces a scanned image's file size — without affecting image quality.

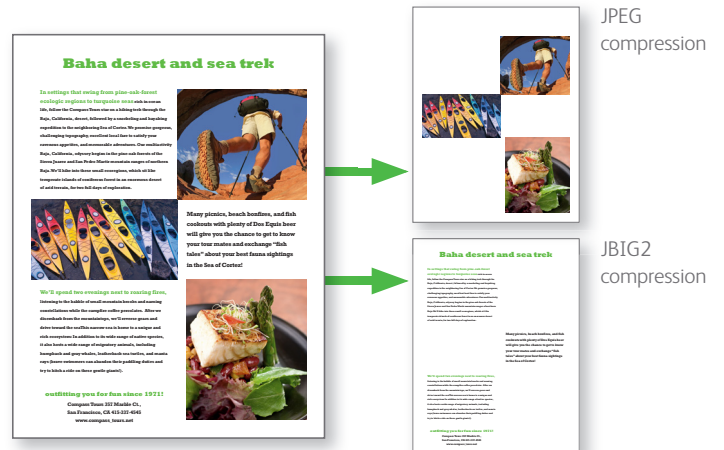
Xerox WorkCentre products* produce scan files that are up to 9 times smaller than those produced by the competition as tested by Industry Analysts, Inc.



* Xerox MFPs tested by Industry Analysts, Inc., include the WorkCentre 7242, WorkCentre 7345, WorkCentre 7675, WorkCentre 5632 and WorkCentre 5675.

The file-size advantage delivered by Xerox means you can create and distribute high-resolution scanned images that contain both text and graphical elements without consuming excessive network bandwidth.

Our products employ the latest image-compression technologies, including the Mixed Raster Content (MRC) method, which splits scanned-file data into separate text and graphic elements. JPEG compression technology is used to compress graphical elements, while JBIG2 is used to compress text elements.



The Xerox MRC image compression method splits a single scan into separate text and graphics components for optimized compression of each element.

On devices with scanning functionality, will the installer or repair person ensure that a one-page instructional flyer is posted at the device that explains why OCR is critical to make PDFs accessible to people with disabilities and instructs the user how to easily turn the OCR capability on/off? Please explain

Yes, we can print and mount a sign at the devices were requested to include the below information. For Searchable PDF in Scan To:

1. Login to the Embedded Web Server.
2. Select Apps.
3. Select Scan To.
4. Scroll Down to Searchable Text and set to On. The Searchable Text selection will apply Optical Character Recognition (OCR) to file formats that support OCR such as PDF. When enabled the output file will include text based information derived from the scanned image of text characters.

Scroll Down to Searchable Text Compression and set to On. Searchable Text Compression is only applicable when Searchable Text is enabled. When Searchable Text and Searchable Text Compression are both turned on along with a compatible file format (PDF, XPS) then the text based information included in the output file will be compressed creating a smaller sized output file.

5. Logout of Embedded Web Server.

How To Enable Optical Character Recognition When Scanning Documents

Product support for: AltaLink B80XX, AltaLink C80XX, AltaLink B80XX Family, AltaLink C80XX Family

Note: Internet Explorer for Windows and Safari for Macintosh are the recommended Internet browsers when accessing the Configuration Site.

1. Open a web browser and enter the IP address of the printer in the address field, then press Enter. Note: You can find the IP address of the machine by pressing the Deviceapp and then the Aboutapp on the printers' user interface.
2. Log-in as an Administrator by pressing the Log-In button.
3. Click on the Properties tab.
4. On the left side of the page click on Apps.
5. Click on Email > Setup.
6. On the right side of the page, under Email Setup, click on Defaults.
7. Under Email Options, click on Edit. This will bring up a set of formats for your files.
8. Under File Options, select the Searchable option to enable it. Note: With this option enabled, scanned documents can now be edited.
9. Click Save.
10. Test by sending a scanned document to yourself.

Note: Enabling this option will make the sizes of your scanned files bigger and this could prevent the ability to scan successfully.



An innovative voice solution supporting workers of all abilities.

Language is an effective means of communication.

"Gabi, make 10 color copies, double-sided, and stapled."

Gabi Voice allows workers of all abilities to access their multifunction printer's copying, scanning, faxing, and secure printing functions using their voice. The device is controlled using natural language and simple commands including a request for service.

gabi | voice

Why Gabi Voice?

Ensure legislative requirements: Gabi Voice is 508c compliant for use by employees with disabilities.

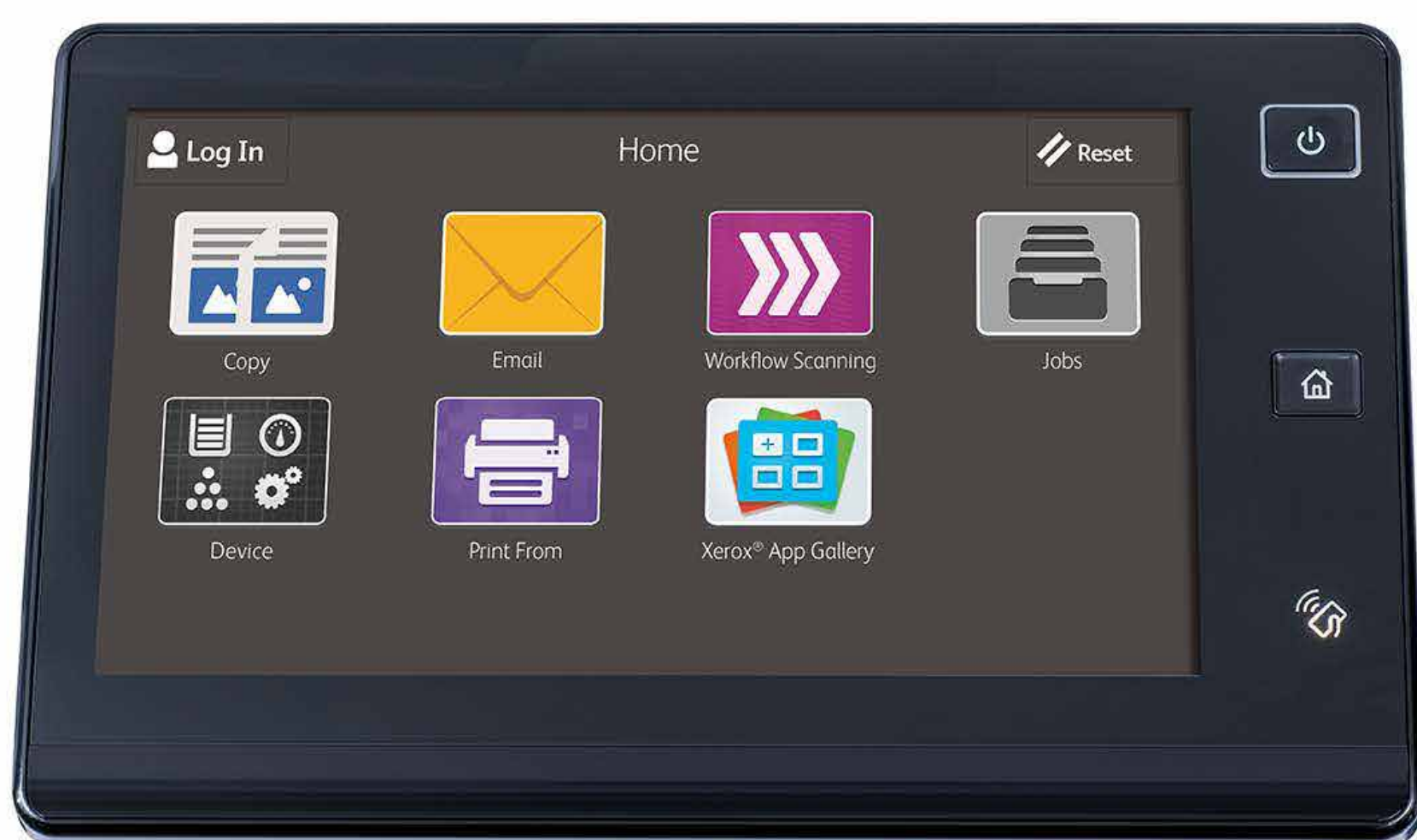
Enable workplace independence: No commands to memorize. Basic commands are spoken in any order for the desired outcome.

Increase productivity: Voice commands save time. No need for manuals, icons, or menus.

Stay secure: Powered by IBM Watson, Gabi voice commands are interpreted securely and accurately. No personal information is exchanged or stored with this solution.

Gabi Voice is convenient: Place a service call while at the device. Gabi gathers the pertinent service information along with your serial number and emails your service provider.

Currently utilizing English-only commands, Gabi can help with conveying toner and paper levels before performing large jobs.



Current Xerox® Devices Supported:

- Xerox® AltaLink® C8030/C8035/C8045/C8055/C8070
- Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090

These key multifunction printer features are supported with Gabi Voice:

- Copy
- Scan to Email
- Fax
- Secure Print
- Device - to submit a service request

Components

1-to-1 Gabi Smartbox: Ethernet/USB/Bluetooth equipped micro-controller device designed to communicate directly with the MFP.

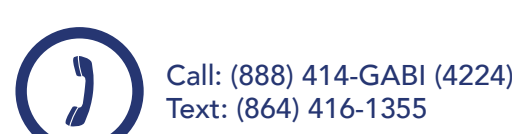
Speaker: An on-premises dedicated and integrated microphone/speaker that aids the user in communication via voice. Connected directly to the Gabi Smartbox via USB.

Power: 5.1V micro USB power adapter UL approved.

Engage our voice recognition solution by using the wake-up word, "gabi."

Gabi Voice is not just a name, but a Global Artificial Business Intelligence platform for the printing industry complying with 508c standards. Powered by the cognitive brain of IBM Watson, Gabi enables hands-free access to your multifunction printer.

To learn more about Gabi Voice and Gabi Solutions, visit www.gabisolutions.com





Gabi Voice

Customer Expectations Document
For Xerox® AltaLink family

Document version: 27April 2020

Gabi Gov Customer Expectation Document Table of Contents

ABOUT THIS DOCUMENT	3
PRODUCT DESCRIPTION	3
CAPABILITIES OF GABI VOICE	3
PRODUCT HARDWARE	3
PRE-REQUISITES	4
TERMINOLOGY	4
INSTALLATION	4
USER INTERACTION	4
PROCESS FLOW	4
AVAILABLE INTENTS	5
COPY	5
SCAN TO EMAIL	5
SERVER FAX	6
SECURE PRINT	7
MACHINE STATUS	7
SUPPLY LEVELS	7
INQUIRIES	8
TECHNOLOGY PARTNERS	8
INSTALLATION SUPPORT	8
MAINTENANCE SUPPORT	8
ERROR HANDLING	8
SUPPORT	9
APPENDIX A	10

ABOUT THIS DOCUMENT

The purpose of this document is to set customer expectations of the Gabi Voice workflows and any associated caveats related to the Xerox AltaLink family. In addition, this document includes reference to the Service Subscription Agreement required to understand Gabi Voice Solution (APPENDIX A).

Please read this document in its entirety. It contains important information that will help ensure a smooth operating experience with Gabi Voice.

Please note: Completing the Configuration Worksheet is the single most important step for ensuring successful enablement of the Gabi Voice solution. The Configuration Worksheet available on TXC is required before placing orders for Gabi Voice Solution with your Xerox authorized sales rep. The configuration information needs to be sent to support@gabisolutions.com as soon as your purchase of the Gabi Voice system is processed with Xerox via TXC.

PRODUCT DESCRIPTION

English only

Gabi Voice provides a touchless voice user interface for interfacing with a Xerox AltaLink Multifunction printer (MFP).

The voice user interface is structured via natural language input and adapts to variances based on user speech patterns. As the input is detected from the conversation, a corresponding set of machine executable commands are derived from a database whitelist of known functions. Gabi Voice will only perform actions that have been pre-programmed, which will be covered later in this document. The Gabi Voice solution is designed to be an on-premises device that securely interfaces with IBM Watson © once the wake-word has been invoked and language commands have been supplied..

CAPABILITIES OF GABI VOICE

The following multifunction printer functions are enabled with Gabi Voice.

- Copy
- Email
- Server Fax
- Secure Print Release¹
- Machine Status
- Inquiries²

¹ Secure Print Release requires external keyboard for pin entering

² Please check with your Sales Representative to determine if Service Ticket Assistance is supported. GabiVoice is not supported with any Xerox Service Contract, all support is provided via GabiSolutions.

Gabi Voice is not supported on Xerox FSMA Service contracts.

Gabi Voice does not support any 3rd Party Authentication Solutions, XWS, XDM, XDA.

PRODUCT HARDWARE

Contents provided with Gabi Voice include:

- Smartbox appliance
- Power supply
- Talk to Me Speaker/Microphone

Note: An ethernet cable is not included. Gabi Voice supports IPV4 and IPV6 environments.

PRE-REQUISITES

1. Gabi Voice Solution requires a separate physical dedicated Ethernet port and power outlet from the MFP.
2. Customer required to supply an Ethernet Cable that will enable connection between the Smartbox and Network drop..
3. The Xerox AltaLink device firmware must be at level 100.XXX.028.05200 or higher. This firmware can be found on the AltaLink configuration sheet or on the Local User Interface device icon.
4. Scan to fax feature requires Gabi Voice to be in a Server Fax enabled environment.
5. Secure Print Release may require the optional USB keyboard. Contact Xerox Customized Application Solutions or your Xerox Sales Representative for more information.

TERMINOLOGY

Intent: Expected goal to be achieved.

Entity: An item, term, or object that provides context to the intent.

Wake-word: A word said aloud to start the microphone recording service. Throughout the document when mentioning the wake-word, it is assumed the user is saying "gabi."

VUI: Voice User Interface.

INSTALLATION

Setup for Gabi Solutions requires AltaLink Administration Log-in access. A customer Administrator should reference the Gabi Voice Technology Overview and Installation Guide prior to connecting Gabi to the MFP.

USER INTERACTION

To initiate Gabi Voice the user can invoke the wake-word "Hey Gabi" along with the intended command. The Wake word systematically triggers release of the microphone from a non-recording state and places into an active recording stream. The recording stream remains active until it detects a natural pause in the conversation.

After the command is detected, Gabi invokes a sub process to determine if the minimum parameters have been supplied. If additional options are required, a conversation dialog will be initiated to gather more input from the user.

At any time, a user can simply say "Cancel" to break out of the dialog and return to the default home/idle state. Any errors encountered on the device during user interaction will be reported back verbally if the requested intent could not be completed successfully.

PROCESS FLOW

Along with the Gabi conversation the Speaker/Microphone is equipped with LED lights to provide a visual feedback.

- Device thinking state, led bars will flash
- Microphone is activated and listening, led bars are solid green
- Error occurrence (Gabi Voice or Device), led bars are solid red

AVAILABLE INTENTS

COPY

Entities: Quantity (1-50), Sides (Double-sided or Single-sided), Color (Full Color, Black and White or Auto Detect Color)

Caveats:

Leveraging copy functionality by an external application such as Gabi Voice is only made possible in Xerox proprietary EIP 4.0. Settings for EIP 4.0 are described in the install guide.

Copy function does not support the following:

- Booklet making, C/Z-folding and hole punching are not supported
- Layout adjustments and Job Assembly functions are not supported

Example Flow:

User - "Hey Gabi [pause for beep] Make a Copy."

Gabi - "Your Job will now begin."

To access your MFP's additional options for making a copy, you'll need to add these values at the end of your command as shown in the below example interaction.

User - "Hey Gabi [pause for beep] Make a Single Sided Copy."

Gabi - "Your Job will now begin."

SCAN TO EMAIL

The email is sent to the recipient directly from the device using the SMTP settings as defined locally.

Entities: Gabi will decipher from the user input first name, last name, email address. If a name is supplied with multiple entries in the device address book, the user will be prompted to confirm the correct entry.

For example: Gabi will say: Say 1 for Mark Jacobs ... Say 2 for Marc Simpson

Caveats:

- If the device address book is unavailable due to permission restrictions, then it will not be queryable for user selection.
- If MFP has an active session logged-in at the local user interface then an error "The device is busy" will be reported by Gabi Voice. This is a known limitation of EIP and will be addressed with a future patch provided by Xerox®.
- The Email application does not support the following:
 - Not all scan file formats – PDF is the default
 - Build Job is not supported
 - Layout adjustments and job assembly functions are not supported

Note: Changes to the address book - additions and deletions - will require an export of the address book. Consult the Gabi Voice Installation Guide for more

Example Flow:

User - "Hey Gabi [pause for beep] Scan to Email."

Gabi - "Now checking for logged in users to email. I could not find a logged in user's email. Who would you like to email?"

User - "Bruno Silva"

Gabi - "Now searching the address book. Do you want to email Bruno Silva?"

User - "Yes"

Gabi - "Okay, would you like to set any additional options?"

User - "Yes"

Gabi - "Which option would you like to set? Say ' I need help' for a list of options or help me with setting and [Option Name] "

User - "I need help."

Gabi - "Options are sides, color, resolution, original type, paper size, orientation, lighten, darken, searchable text, background suppression, subject

line and file attachment name. To set, say Set [Option Name] to [Value] ."

SERVER FAX

Server fax is only supported at this time. Using the Gabi VUI, a user can construct a scan job ticket with the purpose of setting the destination to be a fax recipient. If the user is currently logged-in at the time, then the session will be associated with the process.

The fax is sent to the recipient directly from the device using the fax communication settings as defined locally.

Example Invocations:

- Hey Gabi [pause for beep] Send a Fax
- Hey Gabi [pause for beep] Send a Fax to Jane Doe
- Hey Gabi [pause for beep] Send a Fax using my keyboard

Entities:

- Contact Name
- Fax Number
- Sides (Double-sided, or Single-Sided)
- Color (Black and White, Full Color or Auto Detect Color)
- Paper Size (Letter, Legal or Mixed)
- Original Type (Printed Original, Inkjet Original, Solid Ink Original or Photocopied Original)
- Resolution (50%, 75%, 100%, 125%, 150% or 200%)
- Darken (50% or 100%)
- Lighten (50% or 100%)

Gabi will decipher from the user input first name, last name, fax number.

If a name is supplied and multiple entries exist in the device address book, then the user will be prompted to confirm the correct entry.

For example:

Gabi will say: Say 1 for Mark Jacobs ... Say 2 for Marc Simpson

Reference Gabi Voice User Guide for more detail.

Caveats:

- If the device address book is unavailable due to permission restrictions, then it will not be queryable for user selection.
- If MFP has an active session logged-in at the local user interface then an error "The device is busy" will be reported by Gabi Voice. This is a known limitation of EIP and will be addressed with a future patch provided by Xerox® .

- It is the responsibility of the user engaged in the Voice User Interface to supply a valid fax number in accordance with the dialing restrictions of the environment. Gabi Voice will not attempt to parse or format the number any differently than how it was provided by the user.
- The Fax application does not support the following:
 - Cover sheet
 - Contrast adjustment
 - Layout adjustment
 - Starting rate, delay send, email confirmation, fax cover sheet, job assembly, etc.
 - Fax mask data is not supported. No special character support.

Note: Changes to the MFP's address book - additions and deletions - will require an export of the address book. Consult the Gabi Voice Installation Guide for more details.

SECURE PRINT

Allows a user to release secure print jobs from the queue. When invoked, the user will be asked to enter their pin via an external USB keypad (not supplied). Any jobs matching the logged-in user id will be automatically released.

Due to confidentiality of the file names, no job names will be read out loud. Entities:

Entities:

- Secure Print Type (Release or Delete)
- PIN Number

Caveats:

- The MFP must be at a minimum firmware level of 100.XXX.028.05200 . Otherwise jobs cannot be released.
- The PIN code can only be read from an external keyboard. The on-board soft-keyboard cannot communicate with Gabi Voice. While we support most external USB keyboards, it is recommended to use the Xerox ® T00015 accessibility keyboard.

MACHINE STATUS

Allows a user to retrieve machine status as it would be displayed on the walk-up screen, i.e. "Tray 4 is empty, Machine is in sleep mode, etc..."

Entities: None

Caveats: None

Example Invocation:

- Hey Gabi [pause for beep] What is the status of my device?
- Hey Gabi [pause for beep] What is the status of my machine?

SUPPLY LEVELS

Allows user to query the MFP to determine paper and toner levels

Example Invocations:

- Hey Gabi [pause for beep] What are my paper levels?
- Hey Gabi [pause for beep] What are my toner levels?

Entities: None

Caveats: SNMP must be enabled as a service on the MFP for this to operate correctly. In addition, the public community string must be configured if different from default.

INQUIRIES

Not supported on Xerox Service contracts, check with your Sales Representative.

Allows a user to submit a service request to a predetermined endpoint. In the event of a service request, any available diagnostics are collected along with the message body.

All Service Support is provided by Gabi Solutions. Contact Gabi Solutions to set up the service request option support@gabisolutions.com

TECHNOLOGY PARTNERS

Gabi is made possible in part due to the partnership with IBM Watson AI cognitive platform to leverage advanced natural language processing.

Gabi also leverages AWS GovCloud for powering its underlying API. AWS GovCloud (US) is an isolated AWS region designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) Region adheres to U.S. International Traffic in Arms Regulations (ITAR) requirements.

INSTALLATION SUPPORT

The Gabi Voice system is customer installable. Installation support for Gabi only is provided by the Gabi Voice hotline support@gabisolutions.com. Please contact the Xerox Authorized Service representative for issues related to AltaLink.

MAINTENANCE SUPPORT

The customer should contact the Gabi Solutions support@gabisolutions.com for any problems, issues or questions with the Gabi Voice Solution.

Enhancements, patches, and security updates may periodically be required. Please leave Gabi on-line to received updates.

AltaLink issues should be directed to a Xerox Authorized Service provider. For help in determining if issues are AltaLink or Gabi Solutions please reference Xerox Support <https://www.support.xerox.com/> and use key word "Gabi" for instructions.

ERROR HANDLING

The Gabi Smartbox is designed to propagate errors encountered during interaction back to the user. These errors include:

- Operational errors that prohibit the device from working properly, i.e. paper tray open
- User defined errors, such as invoking an unrecognized whitelisted Gabi Voice command
- Device service error, such as an authentication error, that prohibit the request from being fulfilled

Gabi Voice will not report errors if there is no activity performed by the user.



300 John St., Suite 1B, Greer, SC 29651
888-414-GABI (4224)
www.GabiSolutions.com

SUPPORT

For issues with Gabi, please feel free to contact Gabi Solutions at support@gabisolutions.com or (888)611-2679 between 8:00-5:00 PM EST

APPENDIX A

Subscription Services AGREEMENT

Note: This is for customer information only. As part of the Gabi Voice enablement process customers will be asked to accept this agreement directly with Gabi Solutions.

GABI VOICE SUBSCRIPTION SERVICES AGREEMENT

This Gabi Voice Subscription Services Agreement (“Agreement”) is by and between InField Sales Pro, LLC, d/b/a Gabi Solutions (“Gabi”) and Customer and is effective on the date Hardware is delivered to Customer for use with a multifunction printer provided by Xerox Corporation (“MFP”) (“Effective Date”). Whereas, Gabi provides a subscription Service, Customer desires to subscribe to the Service, and this business relationship and the allocation of responsibilities regarding such Service are set forth in this Agreement. Therefore, the parties agree as follows:

1. Customer’s Use of the Service.

1.1 Provision of the Service. In exchange for the fees paid as contemplated herein, Gabi shall: (i) make the Service available in accordance with the Documentation and the SLA to Customer and its Enabled Users in the Field of Use during the Term pursuant to this Agreement; (ii) not use Customer Data except to provide the Service, or to prevent or address service or technical problems, in accordance with this Agreement and the Documentation, or in accordance with Customer’s instructions; and (iii) not disclose Customer Data to any third party. The Service is provided in U.S. English. Gabi has translated portions of the Service into other languages. Customer and its Enabled Users may only use the translated portions of the Service for the number of languages listed in an applicable Order Form. Gabi will provide support in accordance with Exhibit A, which is included at no additional charge to Customer; or at Customer’s option and upon payment of applicable fees, Gabi will provide enhanced support in accordance with Exhibit B.

1.2 Customer Obligations. Customer may enable access of the Service for use only by Enabled Users solely for the internal business purposes of Customer and its Affiliates in accordance with the Documentation and not for the benefit of any third parties. Customer is responsible for all Enabled User use of the Service and compliance with this Agreement. Customer shall: (a) have sole responsibility for promptly installing updates to the Service, and for the accuracy, quality, and legality of all Customer Data; and (b) prevent unauthorized access to, or use of, the Service, and notify Gabi promptly of any such unauthorized access or use. Customer shall not: (i) use the Service in violation of applicable Laws; (ii) in connection with the Service, send or store infringing, obscene, threatening, or otherwise unlawful or tortious material, including material that violates privacy rights; (iii) send or store Malicious Code in connection with the Service; (iv) interfere with or disrupt performance of the Service or the data contained therein; or (v) attempt to gain access to the Service or its related systems or networks in a manner not set forth in the Documentation. Customer shall designate a maximum number of named contacts to request and receive support services from Gabi (“Named Support Contacts”). Named Support Contacts must be designated to assist with Product(s) for which they initiate support requests.

1.3 Federal Government End Use Provisions (if applicable). Gabi provides the Service, including related Software and technology, for federal government end use solely in accordance with the following: Government technical data and software rights related to the Service include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202.3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a “need for” right not conveyed under these terms, it must

negotiate with Gabi to determine whether there are acceptable terms for transferring additional rights. A mutually acceptable addendum specifically conveying such rights must be executed by the parties in order to convey such rights beyond those set forth herein.

2. Fees.

2.1 Invoices & Payment. Any fees for the Service after the initial five (5) years of the Term, or for any modifications or enhancements to the Service during the Term, will be invoiced in accordance with the relevant Order Form. Except as otherwise set forth in an Order Form executed by Gabi and Customer, all fees due hereunder (except fees subject to good faith dispute) shall be due and payable within thirty (30) days of invoice date. Except as otherwise stated in an Order Form, all fees are quoted and payable in United States dollars and are based on Service rights acquired under this Agreement. Customer shall provide Gabi with complete and accurate billing and contact information including a valid email address for receipt of invoices. Upon Gabi's request, Customer will make payments via wire transfer.

2.2 Non-cancelable & non-refundable. Except as specifically set forth to the contrary under Section 6.2 "Warranty Remedies", Section 7.1 "Indemnification by Gabi", Section 9.2 "Termination", and under the SLA, all payment obligations under any and all Order Forms are non-cancelable and all payments made are non-refundable.

2.3 Non-Payment and Suspension of Service. If Customer's account is more than thirty (30) days past due (except with respect to charges subject to a reasonable and good faith dispute), in addition to any other rights or remedies it may have under this Agreement or by Law, Gabi reserves the right to suspend the Service upon thirty (30) days written notice, without liability to Customer, until such amounts are paid in full.

2.4 Taxes. Except as otherwise stated in an Order Form, Gabi's fees do not include any direct or indirect local, state, federal or foreign taxes, levies, duties or similar governmental assessments of any nature, including value-added, excise, use or withholding taxes (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its acquisitions hereunder, this Agreement, and the Service, excluding U.S. income taxes on Gabi. If Customer has an obligation to withhold any amounts under any Law or tax regime (other than U.S. income tax Law), Customer shall gross up the payments so that Gabi receives the amount actually quoted and invoiced. If Gabi has a legal obligation to pay or collect Taxes for which Customer is responsible under this section, the appropriate amount shall be invoiced to and paid by Customer, unless Customer provides Gabi with a valid tax exemption certificate authorized by the appropriate taxing authority.

2.5 Enabled User Count Verification. In order to manage and improve the Service, Gabi may periodically confirm the number of Enabled User records on its hosted servers.

3. Proprietary Rights.

3.1 Ownership and Reservation of Rights to Gabi Intellectual Property. Gabi and its licensors own all right, title and interest in and to the Service, Documentation, and other Gabi Intellectual Property Rights. Subject to the limited rights expressly granted hereunder, Gabi reserves all rights, title and interest in and to the Service, and Documentation, including all related Intellectual Property Rights. No rights are granted to Customer hereunder other than as expressly set forth herein.

3.2 License Grant. Gabi hereby grants Customer a non-exclusive, non-transferable, right to use the Service and Documentation, solely for the internal business purposes of Customer and Affiliates and solely during the Term, subject to the terms and conditions of this Agreement. Gabi agrees that the Software used by Gabi to provide the Service, coupled with the rights granted to Customer in this section constitutes "intellectual property" as defined in Section 101(35A) of the Bankruptcy Code, as amended, and this Agreement shall be governed by Section 365(n) of the Bankruptcy Code, as applicable, in the event Gabi voluntarily or involuntarily becomes subject to the

protection of the Bankruptcy Code and Gabi or the trustee in bankruptcy rejects the Agreement. In addition, because pursuant to Section 3.4, Customer owns the Customer Data, Gabi shall not list the Customer Data as an asset in any bankruptcy filing, nor shall Gabi identify Customer's Confidential Information as a Gabi asset.

3.3 License Restrictions. Customer shall not (i) modify, copy or create any derivative works based on the Service or Documentation; (ii) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, offer in a service bureau, or otherwise make the Service or Documentation available to any third party, other than to Enabled Users as permitted herein; (iii) reverse engineer or decompile any portion of the Service or Documentation, including but not limited to, any software utilized by Gabi in the provision of the Service and Documentation, except to the extent required by Law; (iv) access the Service or Documentation in order to build any commercially available product or service; or (v) copy any features, functions, integrations, interfaces or graphics of the Service or Documentation.

3.4 Ownership of Customer Data. As between Gabi and Customer, Customer owns Customer Data. Gabi's use of and activities with respect to any Open Source Software in connection with the Service do not and will not provide to any Open Source licensor any rights in Customer Data or any software or other intellectual property owned by or licensed to Customer by third parties.

3.5 Customer Input. Gabi shall have a royalty-free, worldwide, transferable, sub-licensable, irrevocable, perpetual license to use or incorporate into the Service any Customer Input. Gabi shall have no obligation to make Customer Input an Improvement. Customer shall have no obligation to provide Customer Input.

3.6 Aggregated Data Use. Gabi owns the aggregated and statistical data derived from the operation of the Service, including, without limitation, the number of records in the Service, the number and types of transactions, configurations, and reports processed in the Service and the performance results for the Service (the "Aggregated Data"). Nothing herein shall be construed as prohibiting Gabi from utilizing the Aggregated Data for purposes of operating Gabi's business, provided that Gabi's use of Aggregated Data will not reveal the identity, whether directly or indirectly, of any individual or specific data entered by any individual into the Service. In no event does the Aggregated Data include any personally identifiable information; Aggregated Data that is derived, in whole or in part from information that can be identified as being associated with an individual or with a customer shall not be released to any third party unless it has been rendered anonymous in such a way that the data subject is no longer identifiable.

4. Confidentiality.

4.1 Confidentiality. No party shall disclose or use any Confidential Information of the other party except as reasonably necessary to perform its obligations or exercise its rights pursuant to this Agreement and only with the other party's prior written permission. In the event that the receiving party needs to disclose Confidential Information to the disclosing party's employees or Enabled Users to perform its obligations or exercise its rights pursuant to this Agreement, it may do so without prior written permission. Disclosures to third parties (other than Enabled Users) needed to perform obligations or exercise rights pursuant to this Agreement shall not require prior written permission if the third party recipient is subject to a confidentiality obligation that is equal to or more protective than the confidentiality provisions of this Agreement.

4.2 Protection. Without limiting the foregoing, each party agrees to protect the Confidential Information of the other party in the same manner that it protects its own Confidential Information of like kind, but in no event using less than a reasonable standard of care. Confidential Information that is Customer Data shall receive protection in accordance with Section 5 of this Agreement.

4.3 Compelled Disclosure. A disclosure by one party of Confidential Information of the other party to the extent required by Law shall not be considered a breach of this Agreement, provided the party so compelled promptly provides the other party with prior notice of such compelled disclosure (to the extent legally permitted) and provides reasonable assistance, at the other party's cost, if the other party wishes to contest the disclosure.

4.4 Remedies. If a party discloses or uses (or threatens to disclose or use) any Confidential Information of the other party in breach of confidentiality protections hereunder, the other party shall have the right, in addition to any other remedies available, to seek injunctive relief to enjoin such acts without first exhausting the informal resolution or mediation processes described in section 10.11. The parties acknowledge that disclosure of Confidential Information may cause irreparable injury and damages, which may be difficult to ascertain and that remedies other than injunctive relief may be inadequate. In addition, in the event that a party fails to return or certify destruction of Confidential Information upon termination of this Agreement, each party is entitled to seek injunctive relief, including a preliminary injunction and an order of seizure and impoundment under Section 503 of the Copyright Act upon an ex parte application by Disclosing Party to protect and recover its Confidential Information.

4.5 Return or Destruction of Confidential Information. Upon the termination or expiration of this Agreement and at Customer's request, Gabi will return or destroy any and all Customer Confidential Information (excluding Customer Data, which is subject to Section 5) that Gabi is capable of returning or destroying in the ordinary course of Gabi's business, unless legally prohibited from doing so. Gabi shall protect any Customer Confidential Information in accordance with this Agreement for so long as Gabi retains such Customer Confidential Information.

4.6 Access to Customer's Computer Systems. Customer and Enabled Users access the Service through the internet; the Service does not require that Gabi have access to Customer's computer systems. In the unlikely event that the parties identify a situation where Gabi will need access to Customer's computer systems, the parties will execute a separate agreement which specifies the terms for such access.

5. Security

5.1 Protection and Retrieval of PII. Unless otherwise requested and expressly agreed in writing by a Customer and Gabi via an Order Form submitted by such Customer to Gabi pursuant to this Agreement, Gabi Voice's default configuration for SaaS does not store PII on (i) Amazon Web Services, or (ii) IBM Watson, where it opts out of data sharing so that, after executing the given task on the Watson platform, Watson is instructed not to store any data; or (iii) any future SaaS component which Gabi may elect to incorporate or make a part of the Gabi Voice configuration at any time during the Initial Term and any renewal term of this Agreement; During the Term of this Agreement, Gabi shall not store any PII in provisioning Services to Customer or its Enabled Users in connection with Gabi Voice. In the event that Customer requests services from Gabi requiring Gabi to gather and store PII (e.g. multifactor authentication for security), Gabi shall provide means to Customer to access and retrieve such Customer Data pursuant to a properly executed Order Form between Gabi and the Customer.

5.2 Unauthorized Disclosure. If either party believes that there has been a disclosure of unencrypted Customer Data to anyone other than Gabi (a "Security Incident"), such party must promptly notify the other party, but not later than forty-eight hours after identification of the disclosure unless Law enforcement officials have requested or require a delay in notice. Additionally, each party will reasonably assist the other party in remediating or mitigating any potential damage, including any notification which should be sent to individuals impacted or potentially impacted, or the provision of credit reporting services to such individuals. Each party shall bear the costs of such remediation or mitigation to the extent the breach or security incident was caused by it. Where the type of Customer Data disclosed is such that credit reporting services should be part of remediation efforts, unless the party financially responsible for the remediation efforts agrees to a longer period, one year of credit reporting

services shall be provided. Subject to the limitation of liability in Section 8, to the extent that Gabi caused the breach or security incident, Gabi's obligation to bear the costs of such remediation or mitigation shall include the cost of defending or settling third party claims brought against Customer as the result of the breach or security incident.

As soon as reasonably practicable after any such Security Incident, Customer and Gabi will consult in good faith regarding the root cause analysis and any remediation efforts. Following notice from Gabi to Customer of a security incident caused by Gabi, Customer will have the right to request from Gabi a report prepared by a nationally recognized independent third party audit firm of the relevant security and controls and/or, if applicable, a summary report of a penetration test of the application performed by an independent third party demonstrating remediation of material risks to the unauthorized disclosure of Customer Data. Gabi will work in good faith to remediate any material security risks identified in the root cause analysis that are within Gabi's reasonable control.

Except to the extent prohibited by applicable Law, each party shall provide the other party with reasonable notice of and the opportunity to comment on and approve the content of all notices, filings, communications, press releases or reports about an unauthorized disclosure of Customer Data that identify the other party by name prior to any publication or communication thereof to any third party other than legal advisors. Notwithstanding the foregoing, each party may provide notice as required by Law even if the other party has not provided such consent. Nothing herein will prevent Gabi from making disclosures about a security incident generally. Where applicable Law clearly allocates the responsibility for providing notice about a Security Incident to Customer, Gabi agrees that Customer has the sole right to determine: (i) whether or not any notices of a Security Incident are required by Law or regulation; (ii) the recipients of each notice of a Security Incident, including individuals, regulators, Law enforcement agencies, and consumer reporting agencies; and (iii) the contents of each notice.

6. Warranties & Disclaimers.

6.1 Mutual Warranties. Each party represents and warrants to the other that: (i) this Agreement has been duly authorized, executed and delivered and constitutes a valid and binding agreement enforceable against such party in accordance with its terms; (ii) no authorization or approval from any third party is required in connection with such party's execution, delivery or performance of this Agreement; (iii) the execution, delivery and performance of this Agreement does not violate the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound; and (iv), with respect to its activities pursuant to this Agreement, it shall comply with all Laws applicable to it related to data privacy, international communications and the transmission of technical or personal data.

6.2 Gabi Warranties. Gabi hereby warrants and represents that during the Term: (i) the Service shall perform materially in accordance with the Documentation; (ii) the functionality of the Service will not be materially decreased during the Term; (iii) it will use commercially reasonable efforts to prevent the introduction of Malicious Code into the Service (except for any Malicious Code submitted by Customer or its Enabled Users to the Service); Gabi warrants the Hardware to be free from defects for a period of one (1) year from the date of purchase.

6.3 Warranty Remedies. Each party shall promptly remedy its breach of the warranties in Section 6.1 upon receipt of notification of such breach. As Customer's exclusive remedy and Gabi's sole liability for breach of the warranty set forth in Section 6.2 (i), (ii), and (iii): (a) Gabi shall correct the non-conforming Service or replace the defective Hardware at no additional charge to Customer; or (b) in the event Gabi is unable to correct such deficiencies after good-faith efforts, Gabi shall refund Customer amounts paid that are attributable to the defective Service from the date Gabi received such notice. To receive warranty remedies, Customer must promptly report deficiencies in writing to Gabi, but no later than thirty (30) days of the first date the deficiency is identified by Customer. Following expiration of the Hardware warranty, Customer may purchase replacement Hardware units from Gabi or

its authorized reseller for use with the Service provided hereunder in place of any defective Hardware unit, without any additional service or other charge.

6.4 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, GABI MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICE AND/OR RELATED DOCUMENTATION. GABI DOES NOT WARRANT THAT THE SERVICE WILL BE ERROR FREE OR UNINTERRUPTED. THE LIMITED WARRANTIES PROVIDED HEREIN ARE THE SOLE AND EXCLUSIVE WARRANTIES PROVIDED TO CUSTOMER IN CONNECTION WITH THE PROVISION OF THE SERVICE.

7. Indemnification.

7.1 Gabi shall defend, indemnify and hold Customer and its respective officers, directors, successors, assigns, agents, and employees (collectively, the "Customer Indemnified Parties"), harmless against any loss, damage or costs (including reasonable attorneys' fees) in connection with claims, demands, suits, or proceedings ("Claims") made or brought against the Customer Indemnified Parties by a third party alleging that the use of the Product by Customer as contemplated hereunder infringes a copyright, a U.S. patent issued as of the Effective Date, or a trademark of a third party; provided, however, that Customer: (a) promptly gives written notice of the Claim to Gabi; (b) gives Gabi sole control of the defense and settlement of the Claim (provided that Gabi may not settle any Claim unless it unconditionally releases Customer of all liability); and (c) provides to Gabi, at Gabi's cost, all reasonable assistance. Gabi shall not be required to indemnify Customer in the event of: (w) modification of the Service by Customer or Enabled Users in conflict with Customer's obligations or as a result of any prohibited activity as set forth herein; (x) use of the Service in a manner inconsistent with the Documentation; (y) use of the Service in combination with any other product or service not provided by Gabi; or (z) use of the Service in a manner not otherwise contemplated by this Agreement. If Customer is enjoined from using the Service or Gabi reasonably believes it will be enjoined, Gabi shall have the right, at its sole option, to obtain for Customer the right to continue use of the Service or to replace or modify the Service so that it is no longer infringing. If neither of the foregoing options is reasonably available to Gabi, then use of the Service may be terminated at the option of Gabi and Gabi's sole liability shall be to refund any prepaid fees for the Service that were to be provided after the effective date of termination.

8. Limitation of Liability.

8.1 Limitation of Liability.

(a) TO THE MAXIMUM EXTENT PERMITTED BY LAW AND EXCEPT WITH RESPECT TO LIABILITY ARISING FROM (I) GABI'S INDEMNIFICATION OBLIGATIONS; (II) CLAIMS FOR BODILY INJURY OR DEATH OR DAMAGES TO REAL PROPERTY OR TANGIBLE PERSONAL PROPERTY TO THE EXTENT RESULTING FROM WILLFUL OR INTENTIONAL MISCONDUCT OF THE PARTY LIABLE FOR THE DAMAGES AND/OR (III) GABI'S BREACH OF THIS AGREEMENT RESULTING IN UNAUTHORIZED DISCLOSURE OF CUSTOMER DATA AS SET FORTH IN SECTION 8.1(b) BELOW, IN NO EVENT SHALL GABI'S OR GABI'S THIRD PARTY LICENSORS' AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHERWISE, EXCEED SUBSCRIPTION FEES ACTUALLY PAID BY CUSTOMER IN CONSIDERATION FOR GABI'S SERVICE DELIVERY DURING THE IMMEDIATELY PRECEDING TWELVE (12) MONTH PERIOD FOR THE SERVICE FROM WHICH THE CLAIM AROSE (OR, FOR A CLAIM ARISING BEFORE THE SECOND ANNIVERSARY OF THE EFFECTIVE DATE OF THE APPLICABLE ORDER FORM, THE AMOUNT PAID FOR THE FIRST TWELVE MONTH PERIOD).

(b) GABI'S AGGREGATE LIABILITY TO CUSTOMER FOR ITS BREACH OF THIS AGREEMENT RESULTING FROM GABI'S UNAUTHORIZED DISCLOSURE OF UNENCRYPTED CUSTOMER DATA COLLECTED VIA THE SERVICE (A "SECURITY

INCIDENT”) (INCLUDING THE COST TO DEFEND THIRD PARTY CLAIMS CAUSED BY SUCH BREACH) SHALL NOT EXCEED \$1,000,000.

8.2 Damages. IN NO EVENT SHALL GABI HAVE ANY LIABILITY TO CUSTOMER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED, OR FOR ANY LOST PROFITS, LOSS OF USE, COST OF DATA RECONSTRUCTION, COST OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THE SERVICE, INCLUDING BUT NOT LIMITED TO THE USE OR INABILITY TO USE THE SERVICE, ANY INTERRUPTION, INACCURACY, ERROR OR OMISSION, EVEN IF THE PARTY FROM WHICH DAMAGES ARE BEING SOUGHT OR SUCH PARTY’S LICENSORS OR SUBCONTRACTORS HAVE BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. NOTWITHSTANDING THE FOREGOING, THE PARTIES AGREE THAT GABI’S OBLIGATION TO RESTORE CUSTOMER DATA IN ACCORDANCE WITH THE SLA IS NOT AN INDIRECT DAMAGE, WHETHER IN CONTRACT, TORT OR OTHERWISE.

9. Term & Termination.

9.1 Term of Agreement. The term of this Agreement commences on the Effective Date and continues for an initial period of five (5) years and at Customer’s election and payment of the applicable then-current subscription fee stated in the Order Form, for successive one-year annual renewal periods (the “Term”).

9.2 Termination. Customer may terminate use of Services upon written notice to Gabi within three (3) months following the commencement date of any renewal period. Gabi shall not issue any credit for the unused portion of Services. In addition, either party may terminate this Agreement, (i) upon thirty (30) days prior written notice to the other party of a material breach by the other party if such breach remains uncured at the expiration of such notice period; or (ii) immediately in the event the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Customer’s failure to meet its payment obligations when due shall be considered a material breach, authorizing Gabi’s immediate termination of this Agreement. In the event the Agreement is terminated, all Order Forms are simultaneously terminated. Upon any termination by Customer pursuant to this section, Gabi shall refund Customer any prepaid fees for the affected Service that were to be provided after the effective date of termination. Finally, each Gabi Voice unit is associated with an MFP serial number. In the event the Customer no longer owns or controls the MFP with which Gabi Voice is installed, Gabi shall have no further obligation under this Subscription Services Agreement.

9.3 Effect of Termination. Upon any termination of this Agreement, Customer shall, as of the date of such termination, immediately cease accessing and otherwise utilizing the applicable Service and Gabi Confidential Information; and Gabi shall immediately cease accessing and otherwise utilizing Customer Confidential Information and Customer Data. Termination for any reason shall not relieve Customer of the obligation to pay any fees accrued or due and payable to Gabi prior to the effective date of termination. Upon termination for cause by Gabi, all future amounts due under all Order Forms shall be accelerated and become due and payable immediately.

9.4 Surviving Provisions. The following provisions of this Agreement shall not survive and will have no further force or effect following any termination or expiration of this Agreement: (i) subsection (i) of Section 1.1 “Provision of the Service”; (ii) Section 3.2 “License Grant”; and (iii) any Order Form(s). All other provisions of this Agreement shall survive any termination or expiration of this Agreement.

10. General Provisions.

10.1 Relationship of the Parties. The parties are independent contractors. This Agreement does not create nor is it intended to create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. There are no third-party beneficiaries to this Agreement.

10.2 Notices. All notices under this Agreement shall be in writing and shall be deemed to have been given upon: (i) personal delivery; (ii) the third business day after first class mailing; or (iii) the second business day after sending by facsimile with telephonic confirmation of receipt. Notices to Gabi shall be addressed to the attention of its General Counsel, Luis J. Diaz, at the address listed above for Gabi. Notices to Customer shall be addressed to Customer's address on file in accordance with its registration. Each party may modify its recipient of notices by providing notice pursuant to this Agreement.

10.3 Waiver and Cumulative Remedies. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right or any other right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a party at law or in equity.

10.4 Force Majeure. Neither party shall be liable for any failure or delay in performance under this Agreement (other than for delay in the payment of money due and payable hereunder) for causes beyond that party's reasonable control and occurring without that party's fault or negligence, including, but not limited to, acts of God, acts of government, flood, fire, civil unrest, acts of terror, strikes or other labor problems (other than those involving Gabi or Customer employees, respectively), computer attacks or malicious acts, such as attacks on or through the Internet, any Internet service provider, telecommunications or hosting facility. Dates by which performance obligations are scheduled to be met will be extended for a period of time equal to the time lost due to any delay so caused.

10.5 Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of Law or otherwise, without the prior written consent of the other party (which consent shall not be unreasonably withheld). Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Order Forms) without consent of the other party in connection with a merger, acquisition, reorganization, or sale of all or substantially all of its assets provided the assignee has agreed to be bound by all of the terms of this Agreement and all past due fees are paid in full, except that Customer shall have no right to assign this Agreement to a direct Competitor of Gabi. Any attempt by a party to assign its rights or obligations under this Agreement in breach of this section shall be void and of no effect. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

10.6 Governing Law; Waiver of Jury Trial. This Agreement shall be governed exclusively by the internal Laws of the State of New Jersey, without regard to its conflicts of laws rules. No version of the Uniform Computer Information Transactions Act or any substantially similar Law enacted in any jurisdiction (collectively "UCITA") will apply to or govern any license granted or any party's performance under this Agreement, or any of the parties' rights and obligations arising pursuant to this Agreement. The applicable Law will be the Law as it existed prior to the enactment of UCITA. All claims must be brought in the state or federal courts located in Essex County, New Jersey, and each party agrees to these as the exclusive forums and waives any claim of inconvenient forum. EACH PARTY HEREBY WAIVES ANY RIGHT TO A JURY TRIAL IN CONNECTION WITH ANY LITIGATION IN ANY WAY ARISING OUT OF OR RELATING TO THIS AGREEMENT. Before commencing any litigation, except for one seeking injunctive relief, the party commencing litigation must exhaust alternative dispute resolution processes described in section 10.11.

10.7 Export. Each party shall comply with the export Laws and regulations of the United States and other applicable jurisdictions in providing and using the Service. Without limiting the generality of the foregoing, Customer shall not make the Service available to any person or entity that: (i) is located in a country that is subject

to a U.S. government embargo; (ii) is listed on any U.S. government list of prohibited or restricted parties; or (iii) is engaged in activities directly or indirectly related to the proliferation of weapons of mass destruction.

10.8 Insurance. Gabi will maintain during the entire Term of this Agreement, at its own expense, the types of insurance coverage specified below, on standard policy forms and with insurance companies with at least an A.M. Best Rating of A-VII authorized to do business in the jurisdictions where the Gabi Services are to be performed.

(a) Workers' Compensation insurance prescribed by applicable local Law and Employers Liability insurance with limits not less than \$1,000,000 per accident/per employee.

(b) Business Automobile Liability covering all vehicles that Gabi owns, hires or leases with a limit of no less than \$1,000,000 (combined single limit for bodily injury and property damage) for each accident.

(c) Commercial General Liability insurance including Contractual Liability Coverage, with coverage for products liability, completed operations, property damage and bodily injury, including death, with an aggregate limit of no less than \$2,000,000.

10.9 Miscellaneous. This Agreement, including Exhibit A, Exhibit B, Exhibit C, and all Order Forms, constitutes the entire agreement between the parties with respect to the subject matter hereof. In the event of a conflict, the provisions of an Order Form shall take precedence over provisions of the body of this Agreement and over any other Exhibit or Attachment. This Agreement supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. The enumeration and section headings are used in this Agreement for reference and convenience only and do not have any substantive significance in the construction or interpretation of this Agreement. As used in this Agreement, the word "including" (as well as "include" and "includes") is not limiting and means "including without limitation." This Agreement has been negotiated and no provision shall be construed against either party for the sole reason that it is the drafter of the provision. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to Law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by Law, and the remaining provisions of this Agreement shall remain in effect. Notwithstanding any language to the contrary therein, no terms or conditions stated in a Customer purchase order or in any other Customer order documentation shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void. Gabi may use Customer's name and logo in lists of customers, on marketing materials and on its website with Customer's prior written consent. This Agreement may be executed in counterparts, which taken together shall form one binding legal instrument. The parties hereby consent to the use of electronic signatures in connection with the execution of this Agreement, and further agree that electronic signatures to this Agreement shall be legally binding with the same force and effect as manually executed signatures.

10.10 Publicity. Gabi shall not use Customer's name, logos or trademarks in any written press releases, advertisements and/or marketing materials, or use Customer's name in lists of customers and on its website, including, but not limited to, Gabi's community portal, without the prior written consent of Customer

10.11 Alternative Dispute Resolution. All disputes between the parties arising out of this Agreement or any corresponding Order Form will first be submitted for informal resolution between authorized representatives of Gabi and Customer. Should the parties be unable to obtain a resolution within thirty (30) days after commencement of informal resolution negotiation, or such other time period agreed to in writing by the parties, either Party (the "Complaining Party") shall submit the dispute to non-binding mediation under the auspices of the American Arbitration Association ("AAA") or another mediation organization agreed upon by the parties for

resolution under its rules then in effect, Each Party shall be responsible for its own expenses related to mediation, including attorneys' fees. If the dispute is not resolved within sixty (60) days after its submission to mediation, the Complaining Party may commence litigation in accordance with section 10.6. All statutes of limitations and periods of repose shall be tolled during the informal resolution period and the mediation proceedings. Pending final resolution of any dispute, the Parties shall continue to fulfill their respective obligations hereunder except that either party may exercise termination rights if permitted by this Agreement. This Section shall survive completion or termination of this Agreement, but under no circumstances shall either party be allowed to initiate Alternative Dispute Resolution or court action of any claim or dispute arising out of this Agreement after such period of time as would normally bar the initiation of legal proceedings to litigate such claim or dispute under the Laws of the State of New Jersey. Notwithstanding anything in this Section 10.11, either party may seek injunctive relief at any time.

11. Definitions.

"Affiliate" means any entity which directly or indirectly controls, is controlled by, or is under common control by either party. For purposes of the preceding sentence, "control" means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity.

"Agreement" means this Gabi Voice Subscription Services Agreement, including its Exhibits, and any fully executed Order Form.

"Competitor" means any entity that may be reasonably construed as offering competitive functionality or services to those offered by Gabi. If the parties cannot agree on whether an entity is a Competitor, then the opinion of three (3) financial analysts with adequate knowledge of the human resources and/or financials software and services industry (chosen by mutual agreement of the parties) commissioned at Gabi's sole expense, shall determine such.

"Confidential Information" means (a) any software utilized by Gabi in the provision of the Service and its respective source code; (b) Customer Data; (c) each party's business or technical information, including but not limited to the Documentation, training materials, any information relating to software plans, designs, costs, prices and names, finances, marketing plans, business opportunities or initiatives, organizational restructuring, insurance or health care offerings, personnel, research, development or know-how that is designated by the disclosing party as "confidential" or "proprietary" or the receiving party knows or should reasonably know is confidential or proprietary; and (d) the terms, conditions and pricing of this Agreement (but not its existence or parties).

"Customer Data" means the electronic data or information submitted by Customer or Enabled Users to the Service including any structured or unstructured information (including, without limitation, text, images, data files, and software) provided by Customer for capture, storage, analysis, processing, extraction, retrieval, management, and/or distribution, including any information that can be generated or derived from such information provided by Customer. Customer Data may include PII.

"Customer Input" means suggestions, enhancement requests, recommendations or other feedback provided by Customer and Enabled Users relating to the operation or functionality of the Service.

"Documentation" means Gabi's electronic and hardcopy user guide for the Service, which may be updated by Gabi from time to time, including the Gabi Voice Technology Overview Document version 03-30-18.1 located at <http://www.gabisolutions.com/assets/uploads/Gabi-Voice-Technology-Overview.pdf>. Gabi may modify the Gabi Voice Technology Overview Document from time to time provided that Gabi shall not materially reduce the features and functionality of, and level of support for, the Product.

"Employee" means employees, consultants, contingent workers, independent contractors, Customer authorized visitors, and retirees of Customer and its Affiliates whose active business record(s) are or may be managed by the Service and for which a subscription to the Service has been purchased.

"Enabled User" shall mean each Employee end-user of Customer that is authorized by Customer to access and use a Product identified at Exhibit A following installation by the Customer with an MFP.

"Hardware" shall mean the Gabi SMARTBOX, and the speaker/microphone that accompanies that Service.

"Improvements" means all improvements, updates, enhancements, error corrections, bug fixes, release notes, upgrades and changes to the Service and Documentation, as developed by Gabi and made generally available for Production use without a separate charge to Customers.

"Intellectual Property Rights" means any and all common law, statutory and other industrial property rights and intellectual property rights, including copyrights, trademarks, trade secrets, patents and other proprietary rights issued, honored or enforceable under any applicable Laws anywhere in the world, and all moral rights related thereto.

"Law" means any local, state, national and/or foreign law, treaties, and/or regulations applicable to a respective party.

"Malicious Code" means viruses, worms, time bombs, Trojan horses and other malicious code, files, scripts, agents or programs.

"Order Form" means the separate ordering documents under which Customer modifies or enhances the Gabi Service pursuant to this Agreement that have been fully executed by the parties.

"Open Source Software" shall have the meaning set forth in Section 3.4 of this Agreement.

"PII" or "Personally Identifiable Information" means any information provided by Customer to Gabi or Gabi Voice relating to an identified or identifiable individual, including, but not limited to, social security number or other unique identifier, health or medical information, credit or debit card numbers, bank account numbers or other financial information, driver's license numbers, and other types of sensitive personal information.

"Product" means the Service and related Hardware that allows persons with disabilities to better access a multifunction printer, the Gabi SmartBox that controls the printer/copier and communicates with our cognitive intelligence engine.

"Security Incident" shall have the meaning set forth in Section 5.3 of this Agreement.

"Software as a Service" or "SaaS" or "Service" mean software-based AI and voice-enabled services (collecting, processing, manipulating, transmitting and storing data) provided to Customers by means of a software application or applications hosted remotely by or on behalf of Gabi and further described in the Gabi Subscription Services Agreement to be executed by Customers.

"SLA" means the Gabi Support and Service Level Availability Policy at Exhibit A, which may be updated by Gabi from time to time.

"Subcontractor" means an entity engaged by Gabi to fulfill part or all of its obligations specific to this Agreement and not suppliers or vendors Gabi may engage in general to provide the Service for its general customer population in a manner that is not specific to this Agreement.

"Term" has the meaning set forth in Section 9.1.



gabi | voice

Your Xerox® Voice Recognition Solution

In a commitment to be the vendor of choice for consumers seeking product accessibility, Xerox® and Gabi® Solutions have formed a strategic partnership in support of a 508c solution for your Xerox® Multifunction Printer (MFP).

Powered by IBM Watson®, Gabi Voice allows workers with physical, mental, and learning disabilities within today's workforce to interact with their Xerox® MFP. By using the wake-up word *Hey Gabi*, you can now tell your Xerox® device to make a copy, send an email, fax, and even access secure print functionalities on the device.

Want to learn more?

Why Gabi Voice?

From Social Security Numbers to Credit Card information, the data you run through your Xerox® Multifunction Printer can be extremely sensitive.



Your jobs issued through Gabi Voice are interpreted securely and accurately at all times. Your data is not stored or transmitted to a third party by neither Gabi Solutions nor IBM Watson®.

Gabi Voice complies with Federal 508c compliance terms enabling the visually impaired and those with learning disabilities to use the MFP's features via natural language.



Disabled workers can now vocalize voice commands through Gabi and watch their MFP execute them flawlessly whether it be making a copy, checking your toner levels, and send an E-Mail.

Getting Started with Gabi Voice – What's Included?

When unboxing your Gabi Voice package, you'll receive the following components:

1-to-1 Gabi Smartbox: An Ethernet/USB equipped micro-controller device designed to communicate directly with the MFP.

Speaker: An on-site microphone/speaker that aids the user in communicating vocally with Gabi. This device connects directly to the Gabi Smartbox via USB.

Power: 5.1v micro USB power adapter UL approved to power up your Gabi Smartbox at all times.

To learn more about Gabi Voice, visit www.gabisolutions.com/gabi-voice



300 John Street
Greer, SC 29651



Call (888) 414-GABI (4224)



Support@GabiSolutions.com



Xerox® Adaptable Accessibility Solution

Empowering the blind, visually impaired
and people of all abilities.

To keep your business strong, your employees need to feel empowered to perform their best. The Xerox® Adaptable Accessibility Solution makes that happen. It operates on a standard tablet to leverage users' existing working knowledge of technology tools. Plus, audio talk-back provides work independence for key features like Copy, Scan to Email and Faxing—helping minimize the barriers technology can have for people with disabilities.

Technology created for users of all abilities.

Ensures Legislation Compliance and Security

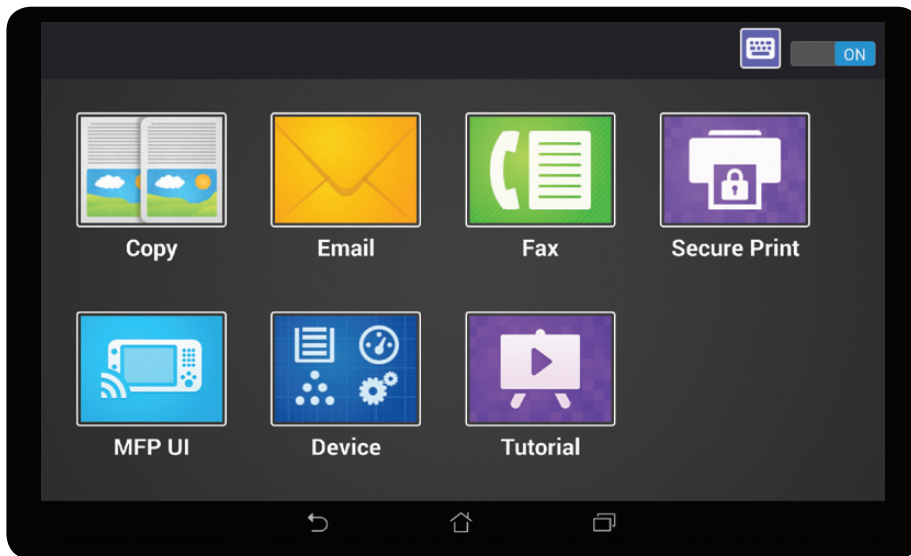
This solution is compliant with the U.S. legislation of the federal Workforce Investment Act of 1998 and amended Section 508 of the Rehabilitation Act. It's integrated with secure solutions like Xerox® Common Access Card authentication for advanced levels of security for sensitive government information. Plus, with Xerox® Secure Print, a unique Pin ID is required for print submission—further enhancing security.

Enhances Workplace Independence

The touch screen of the standard tablet features oversized, easy-to-view application icons for the multifunction features. Combine that with the adjustable mounting bracket that allows them to modify the tablet to their own proper viewing angle—a great flexibility for the visually impaired as well as for those who use wheelchairs. Plus, the USB keyboard provides an easier alternative for data entry for users who prefer this method to navigate through menus and populate fields.

Strengthens Employee Confidence

There are two user modes. User mode one enables audible and talk-back features. That way, blind and visually impaired employees can copy, scan to email and scan with ease. Stress-free accurate task selections can be heard as they are touched on the screen. User mode two displays all features of the multifunction printer user interface. This viewing mode accommodates others using all the solutions and capabilities of the device.



These key multifunction printer features are available with talk-back audio:

- Copy
- Scan to Email
- Fax
- Secure Print Release

Industry-standard tablet

Tutorial available in audio format

Large application icons and touch screen

Robust workflows

- Scan to Email is simple with a local address book on the tablet and USB keyboard.
- Users can scan documents to be turned into searchable PDFs which can be emailed and used with existing technologies providing audible playback.

Of the 15 million visually impaired residents of the United States, nearly 38 percent* are employed. Do you have the resources and tools in place to help them succeed?



Scan this QR code to see how this solution empowers employees at the Association for the Blind and Visually Impaired.

To learn more about the Xerox® Adaptable Accessibility Solution, call your local Xerox sales representative.

*Online Resource for U.S. Disability Statistics. Cornell University. 2013.
©2015 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design®, ConnectKey® and WorkCentre® are trademarks of Xerox Corporation in the United States and/or other countries. BR13804



Touchless Workplace Technologies



Touchless Workplace Technologies

Minimize physical interaction and stay productive with apps for desktop or mobile devices



Workplace Mobile App

Print and scan documents from your mobile devices



Xerox Audio Documents Mobile App

Upload and transform documents into audio files from your tablet or phone



Easy Translator Mobile App and Portal

Translate documents in to 50 different languages instantly



Xerox Proofreader Online Portal

Upload documents and check for plagiarism, grammar, spelling and style using an online portal



Xerox Mobile Link App

Seamlessly connect your Xerox multifunction printer with your mobile device. Open, manipulate, share, and delete scanned or captured documents. Then print, scan or fax with a touch of your mobile device.

Xerox Scan Compression Technology

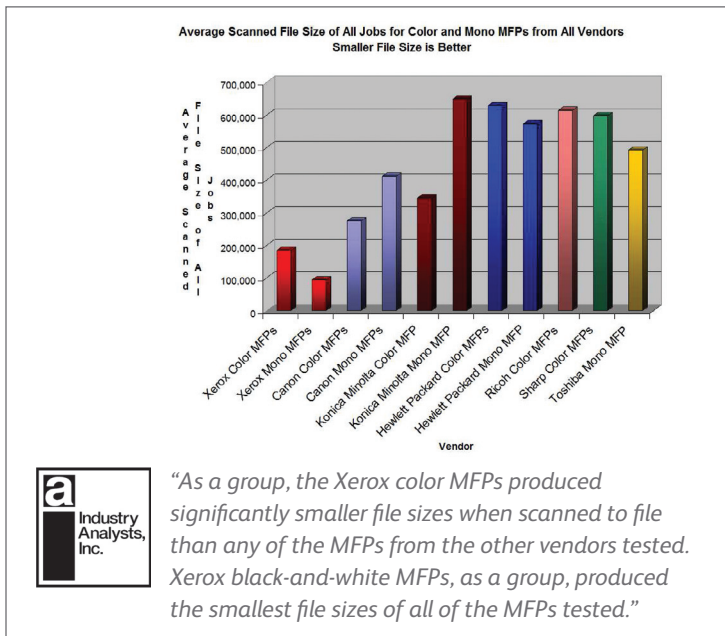
Smaller scan files mean greater office productivity

The power of scanning gives your office more workflow options, making it easy to turn hard copy documents into electronic files for fast distributing, organizing and archiving.

But many popular multifunction devices lack the ability to adequately compress a scanned image, resulting in greater strain on network bandwidth or files with degraded image quality.

Xerox MFPs, however, feature advanced scan-file compression technology that greatly reduces a scanned image's file size — without affecting image quality.

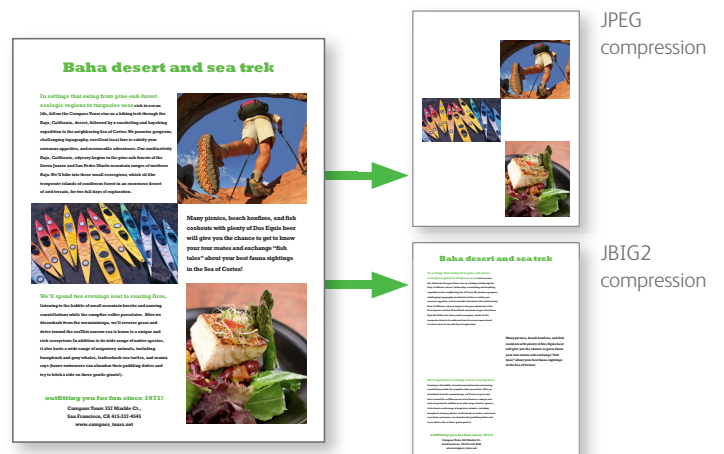
Xerox WorkCentre products* produce scan files that are up to 9 times smaller than those produced by the competition as tested by Industry Analysts, Inc.



* Xerox MFPs tested by Industry Analysts, Inc., include the WorkCentre 7242, WorkCentre 7345, WorkCentre 7675, WorkCentre 5632 and WorkCentre 5675.

The file-size advantage delivered by Xerox means you can create and distribute high-resolution scanned images that contain both text and graphical elements without consuming excessive network bandwidth.

Our products employ the latest image-compression technologies, including the Mixed Raster Content (MRC) method, which splits scanned-file data into separate text and graphic elements. JPEG compression technology is used to compress graphical elements, while JBIG2 is used to compress text elements.



The Xerox MRC image compression method splits a single scan into separate text and graphics components for optimized compression of each element.

On devices with scanning functionality, will the installer or repair person ensure that a one-page instructional flyer is posted at the device that explains why OCR is critical to make PDFs accessible to people with disabilities and instructs the user how to easily turn the OCR capability on/off? Please explain

Yes, we can print and mount a sign at the devices were requested to include the below information. For Searchable PDF in Scan To:

1. Login to the Embedded Web Server.
2. Select Apps.
3. Select Scan To.
4. Scroll Down to Searchable Text and set to On. The Searchable Text selection will apply Optical Character Recognition (OCR) to file formats that support OCR such as PDF. When enabled the output file will include text based information derived from the scanned image of text characters.

Scroll Down to Searchable Text Compression and set to On. Searchable Text Compression is only applicable when Searchable Text is enabled. When Searchable Text and Searchable Text Compression are both turned on along with a compatible file format (PDF, XPS) then the text based information included in the output file will be compressed creating a smaller sized output file.

5. Logout of Embedded Web Server.

How To Enable Optical Character Recognition When Scanning Documents

Product support for: AltaLink B80XX, AltaLink C80XX, AltaLink B80XX Family, AltaLink C80XX Family

Note: Internet Explorer for Windows and Safari for Macintosh are the recommended Internet browsers when accessing the Configuration Site.

1. Open a web browser and enter the IP address of the printer in the address field, then press Enter. Note: You can find the IP address of the machine by pressing the Deviceapp and then the Aboutapp on the printers' user interface.
2. Log-in as an Administrator by pressing the Log-In button.
3. Click on the Properties tab.
4. On the left side of the page click on Apps.
5. Click on Email > Setup.
6. On the right side of the page, under Email Setup, click on Defaults.
7. Under Email Options, click on Edit. This will bring up a set of formats for your files.
8. Under File Options, select the Searchable option to enable it. Note: With this option enabled, scanned documents can now be edited.
9. Click Save.
10. Test by sending a scanned document to yourself.

Note: Enabling this option will make the sizes of your scanned files bigger and this could prevent the ability to scan successfully.



An innovative voice solution supporting workers of all abilities.

Language is an effective means of communication.

"Gabi, make 10 color copies, double-sided, and stapled."

Gabi Voice allows workers of all abilities to access their multifunction printer's copying, scanning, faxing, and secure printing functions using their voice. The device is controlled using natural language and simple commands including a request for service.

gabi | voice

Why Gabi Voice?

Ensure legislative requirements: Gabi Voice is 508c compliant for use by employees with disabilities.

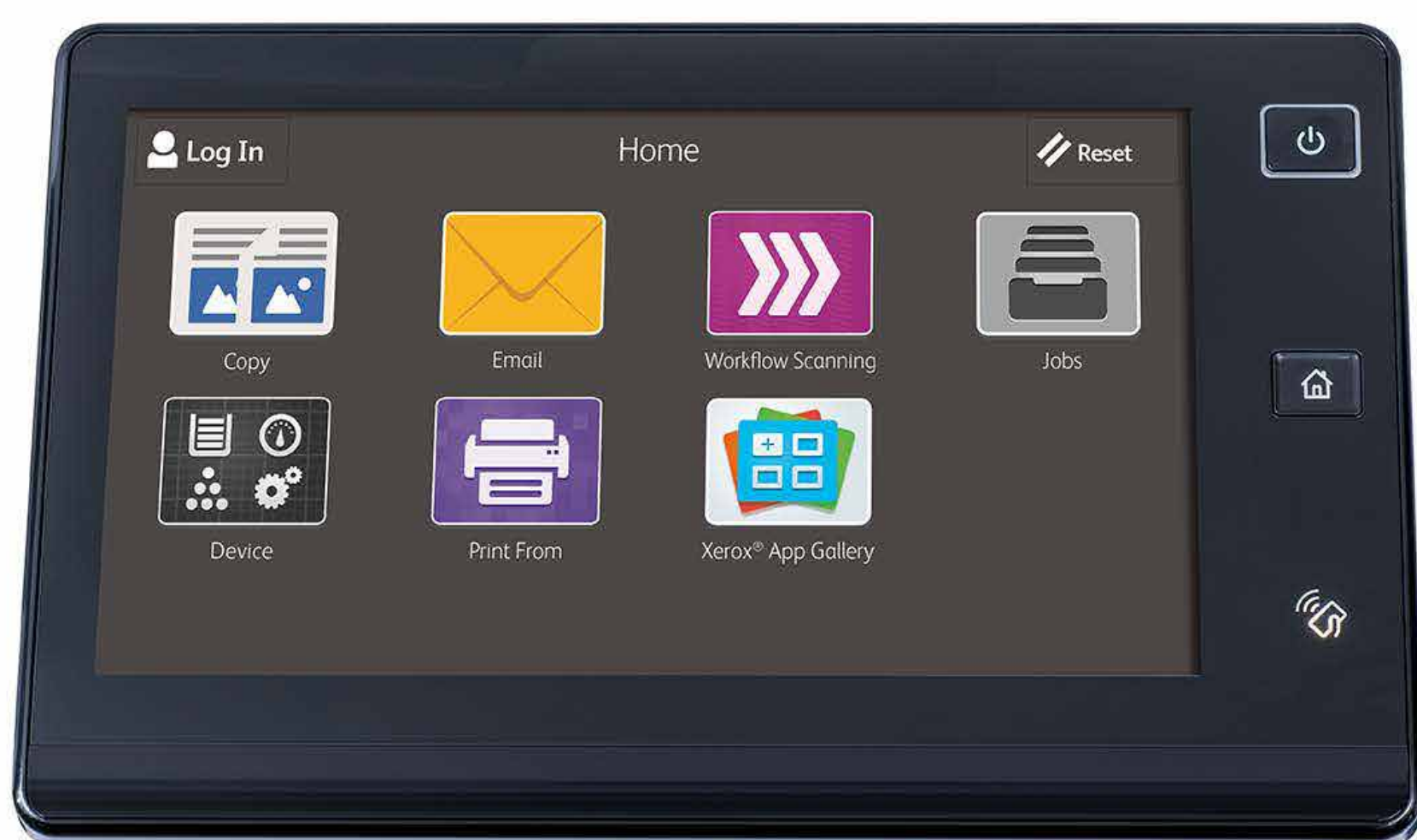
Enable workplace independence: No commands to memorize. Basic commands are spoken in any order for the desired outcome.

Increase productivity: Voice commands save time. No need for manuals, icons, or menus.

Stay secure: Powered by IBM Watson, Gabi voice commands are interpreted securely and accurately. No personal information is exchanged or stored with this solution.

Gabi Voice is convenient: Place a service call while at the device. Gabi gathers the pertinent service information along with your serial number and emails your service provider.

Currently utilizing English-only commands, Gabi can help with conveying toner and paper levels before performing large jobs.



Current Xerox® Devices Supported:

- Xerox® AltaLink® C8030/C8035/C8045/C8055/C8070
- Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090

These key multifunction printer features are supported with Gabi Voice:

- Copy
- Scan to Email
- Fax
- Secure Print
- Device - to submit a service request

Components

1-to-1 Gabi Smartbox: Ethernet/USB/Bluetooth equipped micro-controller device designed to communicate directly with the MFP.

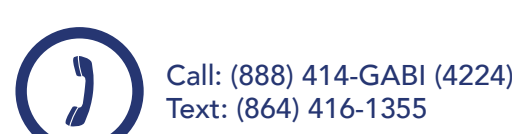
Speaker: An on-premises dedicated and integrated microphone/speaker that aids the user in communication via voice. Connected directly to the Gabi Smartbox via USB.

Power: 5.1V micro USB power adapter UL approved.

Engage our voice recognition solution by using the wake-up word, "gabi."

Gabi Voice is not just a name, but a Global Artificial Business Intelligence platform for the printing industry complying with 508c standards. Powered by the cognitive brain of IBM Watson, Gabi enables hands-free access to your multifunction printer.

To learn more about Gabi Voice and Gabi Solutions, visit www.gabisolutions.com





Gabi Voice

Customer Expectations Document
For Xerox® AltaLink family

Document version: 27April 2020

Gabi Gov Customer Expectation Document Table of Contents

ABOUT THIS DOCUMENT	3
PRODUCT DESCRIPTION	3
CAPABILITIES OF GABI VOICE	3
PRODUCT HARDWARE	3
PRE-REQUISITES	4
TERMINOLOGY	4
INSTALLATION	4
USER INTERACTION	4
PROCESS FLOW	4
AVAILABLE INTENTS	5
COPY	5
SCAN TO EMAIL	5
SERVER FAX	6
SECURE PRINT	7
MACHINE STATUS	7
SUPPLY LEVELS	7
INQUIRIES	8
TECHNOLOGY PARTNERS	8
INSTALLATION SUPPORT	8
MAINTENANCE SUPPORT	8
ERROR HANDLING	8
SUPPORT	9
APPENDIX A	10

ABOUT THIS DOCUMENT

The purpose of this document is to set customer expectations of the Gabi Voice workflows and any associated caveats related to the Xerox AltaLink family. In addition, this document includes reference to the Service Subscription Agreement required to understand Gabi Voice Solution (APPENDIX A).

Please read this document in its entirety. It contains important information that will help ensure a smooth operating experience with Gabi Voice.

Please note: Completing the Configuration Worksheet is the single most important step for ensuring successful enablement of the Gabi Voice solution. The Configuration Worksheet available on TXC is required before placing orders for Gabi Voice Solution with your Xerox authorized sales rep. The configuration information needs to be sent to support@gabisolutions.com as soon as your purchase of the Gabi Voice system is processed with Xerox via TXC.

PRODUCT DESCRIPTION

English only

Gabi Voice provides a touchless voice user interface for interfacing with a Xerox AltaLink Multifunction printer (MFP).

The voice user interface is structured via natural language input and adapts to variances based on user speech patterns. As the input is detected from the conversation, a corresponding set of machine executable commands are derived from a database whitelist of known functions. Gabi Voice will only perform actions that have been pre-programmed, which will be covered later in this document. The Gabi Voice solution is designed to be an on-premises device that securely interfaces with IBM Watson © once the wake-word has been invoked and language commands have been supplied..

CAPABILITIES OF GABI VOICE

The following multifunction printer functions are enabled with Gabi Voice.

- Copy
- Email
- Server Fax
- Secure Print Release¹
- Machine Status
- Inquiries²

¹ Secure Print Release requires external keyboard for pin entering

² Please check with your Sales Representative to determine if Service Ticket Assistance is supported. GabiVoice is not supported with any Xerox Service Contract, all support is provided via GabiSolutions.

Gabi Voice is not supported on Xerox FSMA Service contracts.

Gabi Voice does not support any 3rd Party Authentication Solutions, XWS, XDM, XDA.

PRODUCT HARDWARE

Contents provided with Gabi Voice include:

- Smartbox appliance
- Power supply
- Talk to Me Speaker/Microphone

Note: An ethernet cable is not included. Gabi Voice supports IPV4 and IPV6 environments.

PRE-REQUISITES

1. Gabi Voice Solution requires a separate physical dedicated Ethernet port and power outlet from the MFP.
2. Customer required to supply an Ethernet Cable that will enable connection between the Smartbox and Network drop..
3. The Xerox AltaLink device firmware must be at level 100.XXX.028.05200 or higher. This firmware can be found on the AltaLink configuration sheet or on the Local User Interface device icon.
4. Scan to fax feature requires Gabi Voice to be in a Server Fax enabled environment.
5. Secure Print Release may require the optional USB keyboard. Contact Xerox Customized Application Solutions or your Xerox Sales Representative for more information.

TERMINOLOGY

Intent: Expected goal to be achieved.

Entity: An item, term, or object that provides context to the intent.

Wake-word: A word said aloud to start the microphone recording service. Throughout the document when mentioning the wake-word, it is assumed the user is saying "gabi."

VUI: Voice User Interface.

INSTALLATION

Setup for Gabi Solutions requires AltaLink Administration Log-in access. A customer Administrator should reference the Gabi Voice Technology Overview and Installation Guide prior to connecting Gabi to the MFP.

USER INTERACTION

To initiate Gabi Voice the user can invoke the wake-word "Hey Gabi" along with the intended command. The Wake word systematically triggers release of the microphone from a non-recording state and places into an active recording stream. The recording stream remains active until it detects a natural pause in the conversation.

After the command is detected, Gabi invokes a sub process to determine if the minimum parameters have been supplied. If additional options are required, a conversation dialog will be initiated to gather more input from the user.

At any time, a user can simply say "Cancel" to break out of the dialog and return to the default home/idle state. Any errors encountered on the device during user interaction will be reported back verbally if the requested intent could not be completed successfully.

PROCESS FLOW

Along with the Gabi conversation the Speaker/Microphone is equipped with LED lights to provide a visual feedback.

- Device thinking state, led bars will flash
- Microphone is activated and listening, led bars are solid green
- Error occurrence (Gabi Voice or Device), led bars are solid red

AVAILABLE INTENTS

COPY

Entities: Quantity (1-50), Sides (Double-sided or Single-sided), Color (Full Color, Black and White or Auto Detect Color)

Caveats:

Leveraging copy functionality by an external application such as Gabi Voice is only made possible in Xerox proprietary EIP 4.0. Settings for EIP 4.0 are described in the install guide.

Copy function does not support the following:

- Booklet making, C/Z-folding and hole punching are not supported
- Layout adjustments and Job Assembly functions are not supported

Example Flow:

User - "Hey Gabi [pause for beep] Make a Copy."

Gabi - "Your Job will now begin."

To access your MFP's additional options for making a copy, you'll need to add these values at the end of your command as shown in the below example interaction.

User - "Hey Gabi [pause for beep] Make a Single Sided Copy."

Gabi - "Your Job will now begin."

SCAN TO EMAIL

The email is sent to the recipient directly from the device using the SMTP settings as defined locally.

Entities: Gabi will decipher from the user input first name, last name, email address. If a name is supplied with multiple entries in the device address book, the user will be prompted to confirm the correct entry.

For example: Gabi will say: Say 1 for Mark Jacobs ... Say 2 for Marc Simpson

Caveats:

- If the device address book is unavailable due to permission restrictions, then it will not be queryable for user selection.
- If MFP has an active session logged-in at the local user interface then an error "The device is busy" will be reported by Gabi Voice. This is a known limitation of EIP and will be addressed with a future patch provided by Xerox®.
- The Email application does not support the following:
 - Not all scan file formats – PDF is the default
 - Build Job is not supported
 - Layout adjustments and job assembly functions are not supported

Note: Changes to the address book - additions and deletions - will require an export of the address book. Consult the Gabi Voice Installation Guide for more

Example Flow:

User - "Hey Gabi [pause for beep] Scan to Email."

Gabi - "Now checking for logged in users to email. I could not find a logged in user's email. Who would you like to email?"

User - "Bruno Silva"

Gabi - "Now searching the address book. Do you want to email Bruno Silva?"

User - "Yes"

Gabi - "Okay, would you like to set any additional options?"

User - "Yes"

Gabi - "Which option would you like to set? Say ' I need help' for a list of options or help me with setting and [Option Name] "

User - "I need help."

Gabi - "Options are sides, color, resolution, original type, paper size, orientation, lighten, darken, searchable text, background suppression, subject

line and file attachment name. To set, say Set [Option Name] to [Value] ."

SERVER FAX

Server fax is only supported at this time. Using the Gabi VUI, a user can construct a scan job ticket with the purpose of setting the destination to be a fax recipient. If the user is currently logged-in at the time, then the session will be associated with the process.

The fax is sent to the recipient directly from the device using the fax communication settings as defined locally.

Example Invocations:

- Hey Gabi [pause for beep] Send a Fax
- Hey Gabi [pause for beep] Send a Fax to Jane Doe
- Hey Gabi [pause for beep] Send a Fax using my keyboard

Entities:

- Contact Name
- Fax Number
- Sides (Double-sided, or Single-Sided)
- Color (Black and White, Full Color or Auto Detect Color)
- Paper Size (Letter, Legal or Mixed)
- Original Type (Printed Original, Inkjet Original, Solid Ink Original or Photocopied Original)
- Resolution (50%, 75%, 100%, 125%, 150% or 200%)
- Darken (50% or 100%)
- Lighten (50% or 100%)

Gabi will decipher from the user input first name, last name, fax number.

If a name is supplied and multiple entries exist in the device address book, then the user will be prompted to confirm the correct entry.

For example:

Gabi will say: Say 1 for Mark Jacobs ... Say 2 for Marc Simpson

Reference Gabi Voice User Guide for more detail.

Caveats:

- If the device address book is unavailable due to permission restrictions, then it will not be queryable for user selection.
- If MFP has an active session logged-in at the local user interface then an error "The device is busy" will be reported by Gabi Voice. This is a known limitation of EIP and will be addressed with a future patch provided by Xerox® .

- It is the responsibility of the user engaged in the Voice User Interface to supply a valid fax number in accordance with the dialing restrictions of the environment. Gabi Voice will not attempt to parse or format the number any differently than how it was provided by the user.
- The Fax application does not support the following:
 - Cover sheet
 - Contrast adjustment
 - Layout adjustment
 - Starting rate, delay send, email confirmation, fax cover sheet, job assembly, etc.
 - Fax mask data is not supported. No special character support.

Note: Changes to the MFP's address book - additions and deletions - will require an export of the address book. Consult the Gabi Voice Installation Guide for more details.

SECURE PRINT

Allows a user to release secure print jobs from the queue. When invoked, the user will be asked to enter their pin via an external USB keypad (not supplied). Any jobs matching the logged-in user id will be automatically released.

Due to confidentiality of the file names, no job names will be read out loud. Entities:

Entities:

- Secure Print Type (Release or Delete)
- PIN Number

Caveats:

- The MFP must be at a minimum firmware level of 100.XXX.028.05200 . Otherwise jobs cannot be released.
- The PIN code can only be read from an external keyboard. The on-board soft-keyboard cannot communicate with Gabi Voice. While we support most external USB keyboards, it is recommended to use the Xerox ® T00015 accessibility keyboard.

MACHINE STATUS

Allows a user to retrieve machine status as it would be displayed on the walk-up screen, i.e. "Tray 4 is empty, Machine is in sleep mode, etc..."

Entities: None

Caveats: None

Example Invocation:

- Hey Gabi [pause for beep] What is the status of my device?
- Hey Gabi [pause for beep] What is the status of my machine?

SUPPLY LEVELS

Allows user to query the MFP to determine paper and toner levels

Example Invocations:

- Hey Gabi [pause for beep] What are my paper levels?
- Hey Gabi [pause for beep] What are my toner levels?

Entities: None

Caveats: SNMP must be enabled as a service on the MFP for this to operate correctly. In addition, the public community string must be configured if different from default.

INQUIRIES

Not supported on Xerox Service contracts, check with your Sales Representative.

Allows a user to submit a service request to a predetermined endpoint. In the event of a service request, any available diagnostics are collected along with the message body.

All Service Support is provided by Gabi Solutions. Contact Gabi Solutions to set up the service request option support@gabisolutions.com

TECHNOLOGY PARTNERS

Gabi is made possible in part due to the partnership with IBM Watson AI cognitive platform to leverage advanced natural language processing.

Gabi also leverages AWS GovCloud for powering its underlying API. AWS GovCloud (US) is an isolated AWS region designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements. The AWS GovCloud (US) Region adheres to U.S. International Traffic in Arms Regulations (ITAR) requirements.

INSTALLATION SUPPORT

The Gabi Voice system is customer installable. Installation support for Gabi only is provided by the Gabi Voice hotline support@gabisolutions.com. Please contact the Xerox Authorized Service representative for issues related to AltaLink.

MAINTENANCE SUPPORT

The customer should contact the Gabi Solutions support@gabisolutions.com for any problems, issues or questions with the Gabi Voice Solution.

Enhancements, patches, and security updates may periodically be required. Please leave Gabi on-line to received updates.

AltaLink issues should be directed to a Xerox Authorized Service provider. For help in determining if issues are AltaLink or Gabi Solutions please reference Xerox Support <https://www.support.xerox.com/> and use key word "Gabi" for instructions.

ERROR HANDLING

The Gabi Smartbox is designed to propagate errors encountered during interaction back to the user. These errors include:

- Operational errors that prohibit the device from working properly, i.e. paper tray open
- User defined errors, such as invoking an unrecognized whitelisted Gabi Voice command
- Device service error, such as an authentication error, that prohibit the request from being fulfilled

Gabi Voice will not report errors if there is no activity performed by the user.



300 John St., Suite 1B, Greer, SC 29651
888-414-GABI (4224)
www.GabiSolutions.com

SUPPORT

For issues with Gabi, please feel free to contact Gabi Solutions at support@gabisolutions.com or (888)611-2679 between 8:00-5:00 PM EST

APPENDIX A

Subscription Services AGREEMENT

Note: This is for customer information only. As part of the Gabi Voice enablement process customers will be asked to accept this agreement directly with Gabi Solutions.

GABI VOICE SUBSCRIPTION SERVICES AGREEMENT

This Gabi Voice Subscription Services Agreement (“Agreement”) is by and between InField Sales Pro, LLC, d/b/a Gabi Solutions (“Gabi”) and Customer and is effective on the date Hardware is delivered to Customer for use with a multifunction printer provided by Xerox Corporation (“MFP”) (“Effective Date”). Whereas, Gabi provides a subscription Service, Customer desires to subscribe to the Service, and this business relationship and the allocation of responsibilities regarding such Service are set forth in this Agreement. Therefore, the parties agree as follows:

1. Customer’s Use of the Service.

1.1 Provision of the Service. In exchange for the fees paid as contemplated herein, Gabi shall: (i) make the Service available in accordance with the Documentation and the SLA to Customer and its Enabled Users in the Field of Use during the Term pursuant to this Agreement; (ii) not use Customer Data except to provide the Service, or to prevent or address service or technical problems, in accordance with this Agreement and the Documentation, or in accordance with Customer’s instructions; and (iii) not disclose Customer Data to any third party. The Service is provided in U.S. English. Gabi has translated portions of the Service into other languages. Customer and its Enabled Users may only use the translated portions of the Service for the number of languages listed in an applicable Order Form. Gabi will provide support in accordance with Exhibit A, which is included at no additional charge to Customer; or at Customer’s option and upon payment of applicable fees, Gabi will provide enhanced support in accordance with Exhibit B.

1.2 Customer Obligations. Customer may enable access of the Service for use only by Enabled Users solely for the internal business purposes of Customer and its Affiliates in accordance with the Documentation and not for the benefit of any third parties. Customer is responsible for all Enabled User use of the Service and compliance with this Agreement. Customer shall: (a) have sole responsibility for promptly installing updates to the Service, and for the accuracy, quality, and legality of all Customer Data; and (b) prevent unauthorized access to, or use of, the Service, and notify Gabi promptly of any such unauthorized access or use. Customer shall not: (i) use the Service in violation of applicable Laws; (ii) in connection with the Service, send or store infringing, obscene, threatening, or otherwise unlawful or tortious material, including material that violates privacy rights; (iii) send or store Malicious Code in connection with the Service; (iv) interfere with or disrupt performance of the Service or the data contained therein; or (v) attempt to gain access to the Service or its related systems or networks in a manner not set forth in the Documentation. Customer shall designate a maximum number of named contacts to request and receive support services from Gabi (“Named Support Contacts”). Named Support Contacts must be designated to assist with Product(s) for which they initiate support requests.

1.3 Federal Government End Use Provisions (if applicable). Gabi provides the Service, including related Software and technology, for federal government end use solely in accordance with the following: Government technical data and software rights related to the Service include only those rights customarily provided to the public as defined in this Agreement. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data – Commercial Items) and DFAR 227.7202.3 (Rights in Commercial Computer Software or Computer Software Documentation). If a government agency has a “need for” right not conveyed under these terms, it must

negotiate with Gabi to determine whether there are acceptable terms for transferring additional rights. A mutually acceptable addendum specifically conveying such rights must be executed by the parties in order to convey such rights beyond those set forth herein.

2. Fees.

2.1 Invoices & Payment. Any fees for the Service after the initial five (5) years of the Term, or for any modifications or enhancements to the Service during the Term, will be invoiced in accordance with the relevant Order Form. Except as otherwise set forth in an Order Form executed by Gabi and Customer, all fees due hereunder (except fees subject to good faith dispute) shall be due and payable within thirty (30) days of invoice date. Except as otherwise stated in an Order Form, all fees are quoted and payable in United States dollars and are based on Service rights acquired under this Agreement. Customer shall provide Gabi with complete and accurate billing and contact information including a valid email address for receipt of invoices. Upon Gabi's request, Customer will make payments via wire transfer.

2.2 Non-cancelable & non-refundable. Except as specifically set forth to the contrary under Section 6.2 "Warranty Remedies", Section 7.1 "Indemnification by Gabi", Section 9.2 "Termination", and under the SLA, all payment obligations under any and all Order Forms are non-cancelable and all payments made are non-refundable.

2.3 Non-Payment and Suspension of Service. If Customer's account is more than thirty (30) days past due (except with respect to charges subject to a reasonable and good faith dispute), in addition to any other rights or remedies it may have under this Agreement or by Law, Gabi reserves the right to suspend the Service upon thirty (30) days written notice, without liability to Customer, until such amounts are paid in full.

2.4 Taxes. Except as otherwise stated in an Order Form, Gabi's fees do not include any direct or indirect local, state, federal or foreign taxes, levies, duties or similar governmental assessments of any nature, including value-added, excise, use or withholding taxes (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its acquisitions hereunder, this Agreement, and the Service, excluding U.S. income taxes on Gabi. If Customer has an obligation to withhold any amounts under any Law or tax regime (other than U.S. income tax Law), Customer shall gross up the payments so that Gabi receives the amount actually quoted and invoiced. If Gabi has a legal obligation to pay or collect Taxes for which Customer is responsible under this section, the appropriate amount shall be invoiced to and paid by Customer, unless Customer provides Gabi with a valid tax exemption certificate authorized by the appropriate taxing authority.

2.5 Enabled User Count Verification. In order to manage and improve the Service, Gabi may periodically confirm the number of Enabled User records on its hosted servers.

3. Proprietary Rights.

3.1 Ownership and Reservation of Rights to Gabi Intellectual Property. Gabi and its licensors own all right, title and interest in and to the Service, Documentation, and other Gabi Intellectual Property Rights. Subject to the limited rights expressly granted hereunder, Gabi reserves all rights, title and interest in and to the Service, and Documentation, including all related Intellectual Property Rights. No rights are granted to Customer hereunder other than as expressly set forth herein.

3.2 License Grant. Gabi hereby grants Customer a non-exclusive, non-transferable, right to use the Service and Documentation, solely for the internal business purposes of Customer and Affiliates and solely during the Term, subject to the terms and conditions of this Agreement. Gabi agrees that the Software used by Gabi to provide the Service, coupled with the rights granted to Customer in this section constitutes "intellectual property" as defined in Section 101(35A) of the Bankruptcy Code, as amended, and this Agreement shall be governed by Section 365(n) of the Bankruptcy Code, as applicable, in the event Gabi voluntarily or involuntarily becomes subject to the

protection of the Bankruptcy Code and Gabi or the trustee in bankruptcy rejects the Agreement. In addition, because pursuant to Section 3.4, Customer owns the Customer Data, Gabi shall not list the Customer Data as an asset in any bankruptcy filing, nor shall Gabi identify Customer's Confidential Information as a Gabi asset.

3.3 License Restrictions. Customer shall not (i) modify, copy or create any derivative works based on the Service or Documentation; (ii) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share, offer in a service bureau, or otherwise make the Service or Documentation available to any third party, other than to Enabled Users as permitted herein; (iii) reverse engineer or decompile any portion of the Service or Documentation, including but not limited to, any software utilized by Gabi in the provision of the Service and Documentation, except to the extent required by Law; (iv) access the Service or Documentation in order to build any commercially available product or service; or (v) copy any features, functions, integrations, interfaces or graphics of the Service or Documentation.

3.4 Ownership of Customer Data. As between Gabi and Customer, Customer owns Customer Data. Gabi's use of and activities with respect to any Open Source Software in connection with the Service do not and will not provide to any Open Source licensor any rights in Customer Data or any software or other intellectual property owned by or licensed to Customer by third parties.

3.5 Customer Input. Gabi shall have a royalty-free, worldwide, transferable, sub-licensable, irrevocable, perpetual license to use or incorporate into the Service any Customer Input. Gabi shall have no obligation to make Customer Input an Improvement. Customer shall have no obligation to provide Customer Input.

3.6 Aggregated Data Use. Gabi owns the aggregated and statistical data derived from the operation of the Service, including, without limitation, the number of records in the Service, the number and types of transactions, configurations, and reports processed in the Service and the performance results for the Service (the "Aggregated Data"). Nothing herein shall be construed as prohibiting Gabi from utilizing the Aggregated Data for purposes of operating Gabi's business, provided that Gabi's use of Aggregated Data will not reveal the identity, whether directly or indirectly, of any individual or specific data entered by any individual into the Service. In no event does the Aggregated Data include any personally identifiable information; Aggregated Data that is derived, in whole or in part from information that can be identified as being associated with an individual or with a customer shall not be released to any third party unless it has been rendered anonymous in such a way that the data subject is no longer identifiable.

4. Confidentiality.

4.1 Confidentiality. No party shall disclose or use any Confidential Information of the other party except as reasonably necessary to perform its obligations or exercise its rights pursuant to this Agreement and only with the other party's prior written permission. In the event that the receiving party needs to disclose Confidential Information to the disclosing party's employees or Enabled Users to perform its obligations or exercise its rights pursuant to this Agreement, it may do so without prior written permission. Disclosures to third parties (other than Enabled Users) needed to perform obligations or exercise rights pursuant to this Agreement shall not require prior written permission if the third party recipient is subject to a confidentiality obligation that is equal to or more protective than the confidentiality provisions of this Agreement.

4.2 Protection. Without limiting the foregoing, each party agrees to protect the Confidential Information of the other party in the same manner that it protects its own Confidential Information of like kind, but in no event using less than a reasonable standard of care. Confidential Information that is Customer Data shall receive protection in accordance with Section 5 of this Agreement.

4.3 Compelled Disclosure. A disclosure by one party of Confidential Information of the other party to the extent required by Law shall not be considered a breach of this Agreement, provided the party so compelled promptly provides the other party with prior notice of such compelled disclosure (to the extent legally permitted) and provides reasonable assistance, at the other party's cost, if the other party wishes to contest the disclosure.

4.4 Remedies. If a party discloses or uses (or threatens to disclose or use) any Confidential Information of the other party in breach of confidentiality protections hereunder, the other party shall have the right, in addition to any other remedies available, to seek injunctive relief to enjoin such acts without first exhausting the informal resolution or mediation processes described in section 10.11. The parties acknowledge that disclosure of Confidential Information may cause irreparable injury and damages, which may be difficult to ascertain and that remedies other than injunctive relief may be inadequate. In addition, in the event that a party fails to return or certify destruction of Confidential Information upon termination of this Agreement, each party is entitled to seek injunctive relief, including a preliminary injunction and an order of seizure and impoundment under Section 503 of the Copyright Act upon an ex parte application by Disclosing Party to protect and recover its Confidential Information.

4.5 Return or Destruction of Confidential Information. Upon the termination or expiration of this Agreement and at Customer's request, Gabi will return or destroy any and all Customer Confidential Information (excluding Customer Data, which is subject to Section 5) that Gabi is capable of returning or destroying in the ordinary course of Gabi's business, unless legally prohibited from doing so. Gabi shall protect any Customer Confidential Information in accordance with this Agreement for so long as Gabi retains such Customer Confidential Information.

4.6 Access to Customer's Computer Systems. Customer and Enabled Users access the Service through the internet; the Service does not require that Gabi have access to Customer's computer systems. In the unlikely event that the parties identify a situation where Gabi will need access to Customer's computer systems, the parties will execute a separate agreement which specifies the terms for such access.

5. Security

5.1 Protection and Retrieval of PII. Unless otherwise requested and expressly agreed in writing by a Customer and Gabi via an Order Form submitted by such Customer to Gabi pursuant to this Agreement, Gabi Voice's default configuration for SaaS does not store PII on (i) Amazon Web Services, or (ii) IBM Watson, where it opts out of data sharing so that, after executing the given task on the Watson platform, Watson is instructed not to store any data; or (iii) any future SaaS component which Gabi may elect to incorporate or make a part of the Gabi Voice configuration at any time during the Initial Term and any renewal term of this Agreement; During the Term of this Agreement, Gabi shall not store any PII in provisioning Services to Customer or its Enabled Users in connection with Gabi Voice. In the event that Customer requests services from Gabi requiring Gabi to gather and store PII (e.g. multifactor authentication for security), Gabi shall provide means to Customer to access and retrieve such Customer Data pursuant to a properly executed Order Form between Gabi and the Customer.

5.2 Unauthorized Disclosure. If either party believes that there has been a disclosure of unencrypted Customer Data to anyone other than Gabi (a "Security Incident"), such party must promptly notify the other party, but not later than forty-eight hours after identification of the disclosure unless Law enforcement officials have requested or require a delay in notice. Additionally, each party will reasonably assist the other party in remediating or mitigating any potential damage, including any notification which should be sent to individuals impacted or potentially impacted, or the provision of credit reporting services to such individuals. Each party shall bear the costs of such remediation or mitigation to the extent the breach or security incident was caused by it. Where the type of Customer Data disclosed is such that credit reporting services should be part of remediation efforts, unless the party financially responsible for the remediation efforts agrees to a longer period, one year of credit reporting

services shall be provided. Subject to the limitation of liability in Section 8, to the extent that Gabi caused the breach or security incident, Gabi's obligation to bear the costs of such remediation or mitigation shall include the cost of defending or settling third party claims brought against Customer as the result of the breach or security incident.

As soon as reasonably practicable after any such Security Incident, Customer and Gabi will consult in good faith regarding the root cause analysis and any remediation efforts. Following notice from Gabi to Customer of a security incident caused by Gabi, Customer will have the right to request from Gabi a report prepared by a nationally recognized independent third party audit firm of the relevant security and controls and/or, if applicable, a summary report of a penetration test of the application performed by an independent third party demonstrating remediation of material risks to the unauthorized disclosure of Customer Data. Gabi will work in good faith to remediate any material security risks identified in the root cause analysis that are within Gabi's reasonable control.

Except to the extent prohibited by applicable Law, each party shall provide the other party with reasonable notice of and the opportunity to comment on and approve the content of all notices, filings, communications, press releases or reports about an unauthorized disclosure of Customer Data that identify the other party by name prior to any publication or communication thereof to any third party other than legal advisors. Notwithstanding the foregoing, each party may provide notice as required by Law even if the other party has not provided such consent. Nothing herein will prevent Gabi from making disclosures about a security incident generally. Where applicable Law clearly allocates the responsibility for providing notice about a Security Incident to Customer, Gabi agrees that Customer has the sole right to determine: (i) whether or not any notices of a Security Incident are required by Law or regulation; (ii) the recipients of each notice of a Security Incident, including individuals, regulators, Law enforcement agencies, and consumer reporting agencies; and (iii) the contents of each notice.

6. Warranties & Disclaimers.

6.1 Mutual Warranties. Each party represents and warrants to the other that: (i) this Agreement has been duly authorized, executed and delivered and constitutes a valid and binding agreement enforceable against such party in accordance with its terms; (ii) no authorization or approval from any third party is required in connection with such party's execution, delivery or performance of this Agreement; (iii) the execution, delivery and performance of this Agreement does not violate the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound; and (iv), with respect to its activities pursuant to this Agreement, it shall comply with all Laws applicable to it related to data privacy, international communications and the transmission of technical or personal data.

6.2 Gabi Warranties. Gabi hereby warrants and represents that during the Term: (i) the Service shall perform materially in accordance with the Documentation; (ii) the functionality of the Service will not be materially decreased during the Term; (iii) it will use commercially reasonable efforts to prevent the introduction of Malicious Code into the Service (except for any Malicious Code submitted by Customer or its Enabled Users to the Service); Gabi warrants the Hardware to be free from defects for a period of one (1) year from the date of purchase.

6.3 Warranty Remedies. Each party shall promptly remedy its breach of the warranties in Section 6.1 upon receipt of notification of such breach. As Customer's exclusive remedy and Gabi's sole liability for breach of the warranty set forth in Section 6.2 (i), (ii), and (iii): (a) Gabi shall correct the non-conforming Service or replace the defective Hardware at no additional charge to Customer; or (b) in the event Gabi is unable to correct such deficiencies after good-faith efforts, Gabi shall refund Customer amounts paid that are attributable to the defective Service from the date Gabi received such notice. To receive warranty remedies, Customer must promptly report deficiencies in writing to Gabi, but no later than thirty (30) days of the first date the deficiency is identified by Customer. Following expiration of the Hardware warranty, Customer may purchase replacement Hardware units from Gabi or

its authorized reseller for use with the Service provided hereunder in place of any defective Hardware unit, without any additional service or other charge.

6.4 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, GABI MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICE AND/OR RELATED DOCUMENTATION. GABI DOES NOT WARRANT THAT THE SERVICE WILL BE ERROR FREE OR UNINTERRUPTED. THE LIMITED WARRANTIES PROVIDED HEREIN ARE THE SOLE AND EXCLUSIVE WARRANTIES PROVIDED TO CUSTOMER IN CONNECTION WITH THE PROVISION OF THE SERVICE.

7. Indemnification.

7.1 Gabi shall defend, indemnify and hold Customer and its respective officers, directors, successors, assigns, agents, and employees (collectively, the "Customer Indemnified Parties"), harmless against any loss, damage or costs (including reasonable attorneys' fees) in connection with claims, demands, suits, or proceedings ("Claims") made or brought against the Customer Indemnified Parties by a third party alleging that the use of the Product by Customer as contemplated hereunder infringes a copyright, a U.S. patent issued as of the Effective Date, or a trademark of a third party; provided, however, that Customer: (a) promptly gives written notice of the Claim to Gabi; (b) gives Gabi sole control of the defense and settlement of the Claim (provided that Gabi may not settle any Claim unless it unconditionally releases Customer of all liability); and (c) provides to Gabi, at Gabi's cost, all reasonable assistance. Gabi shall not be required to indemnify Customer in the event of: (w) modification of the Service by Customer or Enabled Users in conflict with Customer's obligations or as a result of any prohibited activity as set forth herein; (x) use of the Service in a manner inconsistent with the Documentation; (y) use of the Service in combination with any other product or service not provided by Gabi; or (z) use of the Service in a manner not otherwise contemplated by this Agreement. If Customer is enjoined from using the Service or Gabi reasonably believes it will be enjoined, Gabi shall have the right, at its sole option, to obtain for Customer the right to continue use of the Service or to replace or modify the Service so that it is no longer infringing. If neither of the foregoing options is reasonably available to Gabi, then use of the Service may be terminated at the option of Gabi and Gabi's sole liability shall be to refund any prepaid fees for the Service that were to be provided after the effective date of termination.

8. Limitation of Liability.

8.1 Limitation of Liability.

(a) TO THE MAXIMUM EXTENT PERMITTED BY LAW AND EXCEPT WITH RESPECT TO LIABILITY ARISING FROM (I) GABI'S INDEMNIFICATION OBLIGATIONS; (II) CLAIMS FOR BODILY INJURY OR DEATH OR DAMAGES TO REAL PROPERTY OR TANGIBLE PERSONAL PROPERTY TO THE EXTENT RESULTING FROM WILLFUL OR INTENTIONAL MISCONDUCT OF THE PARTY LIABLE FOR THE DAMAGES AND/OR (III) GABI'S BREACH OF THIS AGREEMENT RESULTING IN UNAUTHORIZED DISCLOSURE OF CUSTOMER DATA AS SET FORTH IN SECTION 8.1(b) BELOW, IN NO EVENT SHALL GABI'S OR GABI'S THIRD PARTY LICENSORS' AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHERWISE, EXCEED SUBSCRIPTION FEES ACTUALLY PAID BY CUSTOMER IN CONSIDERATION FOR GABI'S SERVICE DELIVERY DURING THE IMMEDIATELY PRECEDING TWELVE (12) MONTH PERIOD FOR THE SERVICE FROM WHICH THE CLAIM AROSE (OR, FOR A CLAIM ARISING BEFORE THE SECOND ANNIVERSARY OF THE EFFECTIVE DATE OF THE APPLICABLE ORDER FORM, THE AMOUNT PAID FOR THE FIRST TWELVE MONTH PERIOD).

(b) GABI'S AGGREGATE LIABILITY TO CUSTOMER FOR ITS BREACH OF THIS AGREEMENT RESULTING FROM GABI'S UNAUTHORIZED DISCLOSURE OF UNENCRYPTED CUSTOMER DATA COLLECTED VIA THE SERVICE (A "SECURITY

INCIDENT”) (INCLUDING THE COST TO DEFEND THIRD PARTY CLAIMS CAUSED BY SUCH BREACH) SHALL NOT EXCEED \$1,000,000.

8.2 Damages. IN NO EVENT SHALL GABI HAVE ANY LIABILITY TO CUSTOMER FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED, OR FOR ANY LOST PROFITS, LOSS OF USE, COST OF DATA RECONSTRUCTION, COST OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THE SERVICE, INCLUDING BUT NOT LIMITED TO THE USE OR INABILITY TO USE THE SERVICE, ANY INTERRUPTION, INACCURACY, ERROR OR OMISSION, EVEN IF THE PARTY FROM WHICH DAMAGES ARE BEING SOUGHT OR SUCH PARTY’S LICENSORS OR SUBCONTRACTORS HAVE BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. NOTWITHSTANDING THE FOREGOING, THE PARTIES AGREE THAT GABI’S OBLIGATION TO RESTORE CUSTOMER DATA IN ACCORDANCE WITH THE SLA IS NOT AN INDIRECT DAMAGE, WHETHER IN CONTRACT, TORT OR OTHERWISE.

9. Term & Termination.

9.1 Term of Agreement. The term of this Agreement commences on the Effective Date and continues for an initial period of five (5) years and at Customer’s election and payment of the applicable then-current subscription fee stated in the Order Form, for successive one-year annual renewal periods (the “Term”).

9.2 Termination. Customer may terminate use of Services upon written notice to Gabi within three (3) months following the commencement date of any renewal period. Gabi shall not issue any credit for the unused portion of Services. In addition, either party may terminate this Agreement, (i) upon thirty (30) days prior written notice to the other party of a material breach by the other party if such breach remains uncured at the expiration of such notice period; or (ii) immediately in the event the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. Customer’s failure to meet its payment obligations when due shall be considered a material breach, authorizing Gabi’s immediate termination of this Agreement. In the event the Agreement is terminated, all Order Forms are simultaneously terminated. Upon any termination by Customer pursuant to this section, Gabi shall refund Customer any prepaid fees for the affected Service that were to be provided after the effective date of termination. Finally, each Gabi Voice unit is associated with an MFP serial number. In the event the Customer no longer owns or controls the MFP with which Gabi Voice is installed, Gabi shall have no further obligation under this Subscription Services Agreement.

9.3 Effect of Termination. Upon any termination of this Agreement, Customer shall, as of the date of such termination, immediately cease accessing and otherwise utilizing the applicable Service and Gabi Confidential Information; and Gabi shall immediately cease accessing and otherwise utilizing Customer Confidential Information and Customer Data. Termination for any reason shall not relieve Customer of the obligation to pay any fees accrued or due and payable to Gabi prior to the effective date of termination. Upon termination for cause by Gabi, all future amounts due under all Order Forms shall be accelerated and become due and payable immediately.

9.4 Surviving Provisions. The following provisions of this Agreement shall not survive and will have no further force or effect following any termination or expiration of this Agreement: (i) subsection (i) of Section 1.1 “Provision of the Service”; (ii) Section 3.2 “License Grant”; and (iii) any Order Form(s). All other provisions of this Agreement shall survive any termination or expiration of this Agreement.

10. General Provisions.

10.1 Relationship of the Parties. The parties are independent contractors. This Agreement does not create nor is it intended to create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. There are no third-party beneficiaries to this Agreement.

10.2 Notices. All notices under this Agreement shall be in writing and shall be deemed to have been given upon: (i) personal delivery; (ii) the third business day after first class mailing; or (iii) the second business day after sending by facsimile with telephonic confirmation of receipt. Notices to Gabi shall be addressed to the attention of its General Counsel, Luis J. Diaz, at the address listed above for Gabi. Notices to Customer shall be addressed to Customer's address on file in accordance with its registration. Each party may modify its recipient of notices by providing notice pursuant to this Agreement.

10.3 Waiver and Cumulative Remedies. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right or any other right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a party at law or in equity.

10.4 Force Majeure. Neither party shall be liable for any failure or delay in performance under this Agreement (other than for delay in the payment of money due and payable hereunder) for causes beyond that party's reasonable control and occurring without that party's fault or negligence, including, but not limited to, acts of God, acts of government, flood, fire, civil unrest, acts of terror, strikes or other labor problems (other than those involving Gabi or Customer employees, respectively), computer attacks or malicious acts, such as attacks on or through the Internet, any Internet service provider, telecommunications or hosting facility. Dates by which performance obligations are scheduled to be met will be extended for a period of time equal to the time lost due to any delay so caused.

10.5 Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of Law or otherwise, without the prior written consent of the other party (which consent shall not be unreasonably withheld). Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Order Forms) without consent of the other party in connection with a merger, acquisition, reorganization, or sale of all or substantially all of its assets provided the assignee has agreed to be bound by all of the terms of this Agreement and all past due fees are paid in full, except that Customer shall have no right to assign this Agreement to a direct Competitor of Gabi. Any attempt by a party to assign its rights or obligations under this Agreement in breach of this section shall be void and of no effect. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

10.6 Governing Law; Waiver of Jury Trial. This Agreement shall be governed exclusively by the internal Laws of the State of New Jersey, without regard to its conflicts of laws rules. No version of the Uniform Computer Information Transactions Act or any substantially similar Law enacted in any jurisdiction (collectively "UCITA") will apply to or govern any license granted or any party's performance under this Agreement, or any of the parties' rights and obligations arising pursuant to this Agreement. The applicable Law will be the Law as it existed prior to the enactment of UCITA. All claims must be brought in the state or federal courts located in Essex County, New Jersey, and each party agrees to these as the exclusive forums and waives any claim of inconvenient forum. EACH PARTY HEREBY WAIVES ANY RIGHT TO A JURY TRIAL IN CONNECTION WITH ANY LITIGATION IN ANY WAY ARISING OUT OF OR RELATING TO THIS AGREEMENT. Before commencing any litigation, except for one seeking injunctive relief, the party commencing litigation must exhaust alternative dispute resolution processes described in section 10.11.

10.7 Export. Each party shall comply with the export Laws and regulations of the United States and other applicable jurisdictions in providing and using the Service. Without limiting the generality of the foregoing, Customer shall not make the Service available to any person or entity that: (i) is located in a country that is subject

to a U.S. government embargo; (ii) is listed on any U.S. government list of prohibited or restricted parties; or (iii) is engaged in activities directly or indirectly related to the proliferation of weapons of mass destruction.

10.8 Insurance. Gabi will maintain during the entire Term of this Agreement, at its own expense, the types of insurance coverage specified below, on standard policy forms and with insurance companies with at least an A.M. Best Rating of A-VII authorized to do business in the jurisdictions where the Gabi Services are to be performed.

(a) Workers' Compensation insurance prescribed by applicable local Law and Employers Liability insurance with limits not less than \$1,000,000 per accident/per employee.

(b) Business Automobile Liability covering all vehicles that Gabi owns, hires or leases with a limit of no less than \$1,000,000 (combined single limit for bodily injury and property damage) for each accident.

(c) Commercial General Liability insurance including Contractual Liability Coverage, with coverage for products liability, completed operations, property damage and bodily injury, including death, with an aggregate limit of no less than \$2,000,000.

10.9 Miscellaneous. This Agreement, including Exhibit A, Exhibit B, Exhibit C, and all Order Forms, constitutes the entire agreement between the parties with respect to the subject matter hereof. In the event of a conflict, the provisions of an Order Form shall take precedence over provisions of the body of this Agreement and over any other Exhibit or Attachment. This Agreement supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by the party against whom the modification, amendment or waiver is to be asserted. The enumeration and section headings are used in this Agreement for reference and convenience only and do not have any substantive significance in the construction or interpretation of this Agreement. As used in this Agreement, the word "including" (as well as "include" and "includes") is not limiting and means "including without limitation." This Agreement has been negotiated and no provision shall be construed against either party for the sole reason that it is the drafter of the provision. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to Law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by Law, and the remaining provisions of this Agreement shall remain in effect. Notwithstanding any language to the contrary therein, no terms or conditions stated in a Customer purchase order or in any other Customer order documentation shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void. Gabi may use Customer's name and logo in lists of customers, on marketing materials and on its website with Customer's prior written consent. This Agreement may be executed in counterparts, which taken together shall form one binding legal instrument. The parties hereby consent to the use of electronic signatures in connection with the execution of this Agreement, and further agree that electronic signatures to this Agreement shall be legally binding with the same force and effect as manually executed signatures.

10.10 Publicity. Gabi shall not use Customer's name, logos or trademarks in any written press releases, advertisements and/or marketing materials, or use Customer's name in lists of customers and on its website, including, but not limited to, Gabi's community portal, without the prior written consent of Customer

10.11 Alternative Dispute Resolution. All disputes between the parties arising out of this Agreement or any corresponding Order Form will first be submitted for informal resolution between authorized representatives of Gabi and Customer. Should the parties be unable to obtain a resolution within thirty (30) days after commencement of informal resolution negotiation, or such other time period agreed to in writing by the parties, either Party (the "Complaining Party") shall submit the dispute to non-binding mediation under the auspices of the American Arbitration Association ("AAA") or another mediation organization agreed upon by the parties for

resolution under its rules then in effect, Each Party shall be responsible for its own expenses related to mediation, including attorneys' fees. If the dispute is not resolved within sixty (60) days after its submission to mediation, the Complaining Party may commence litigation in accordance with section 10.6. All statutes of limitations and periods of repose shall be tolled during the informal resolution period and the mediation proceedings. Pending final resolution of any dispute, the Parties shall continue to fulfill their respective obligations hereunder except that either party may exercise termination rights if permitted by this Agreement. This Section shall survive completion or termination of this Agreement, but under no circumstances shall either party be allowed to initiate Alternative Dispute Resolution or court action of any claim or dispute arising out of this Agreement after such period of time as would normally bar the initiation of legal proceedings to litigate such claim or dispute under the Laws of the State of New Jersey. Notwithstanding anything in this Section 10.11, either party may seek injunctive relief at any time.

11. Definitions.

"Affiliate" means any entity which directly or indirectly controls, is controlled by, or is under common control by either party. For purposes of the preceding sentence, "control" means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity.

"Agreement" means this Gabi Voice Subscription Services Agreement, including its Exhibits, and any fully executed Order Form.

"Competitor" means any entity that may be reasonably construed as offering competitive functionality or services to those offered by Gabi. If the parties cannot agree on whether an entity is a Competitor, then the opinion of three (3) financial analysts with adequate knowledge of the human resources and/or financials software and services industry (chosen by mutual agreement of the parties) commissioned at Gabi's sole expense, shall determine such.

"Confidential Information" means (a) any software utilized by Gabi in the provision of the Service and its respective source code; (b) Customer Data; (c) each party's business or technical information, including but not limited to the Documentation, training materials, any information relating to software plans, designs, costs, prices and names, finances, marketing plans, business opportunities or initiatives, organizational restructuring, insurance or health care offerings, personnel, research, development or know-how that is designated by the disclosing party as "confidential" or "proprietary" or the receiving party knows or should reasonably know is confidential or proprietary; and (d) the terms, conditions and pricing of this Agreement (but not its existence or parties).

"Customer Data" means the electronic data or information submitted by Customer or Enabled Users to the Service including any structured or unstructured information (including, without limitation, text, images, data files, and software) provided by Customer for capture, storage, analysis, processing, extraction, retrieval, management, and/or distribution, including any information that can be generated or derived from such information provided by Customer. Customer Data may include PII.

"Customer Input" means suggestions, enhancement requests, recommendations or other feedback provided by Customer and Enabled Users relating to the operation or functionality of the Service.

"Documentation" means Gabi's electronic and hardcopy user guide for the Service, which may be updated by Gabi from time to time, including the Gabi Voice Technology Overview Document version 03-30-18.1 located at <http://www.gabisolutions.com/assets/uploads/Gabi-Voice-Technology-Overview.pdf>. Gabi may modify the Gabi Voice Technology Overview Document from time to time provided that Gabi shall not materially reduce the features and functionality of, and level of support for, the Product.

"Employee" means employees, consultants, contingent workers, independent contractors, Customer authorized visitors, and retirees of Customer and its Affiliates whose active business record(s) are or may be managed by the Service and for which a subscription to the Service has been purchased.

"Enabled User" shall mean each Employee end-user of Customer that is authorized by Customer to access and use a Product identified at Exhibit A following installation by the Customer with an MFP.

"Hardware" shall mean the Gabi SMARTBOX, and the speaker/microphone that accompanies that Service.

"Improvements" means all improvements, updates, enhancements, error corrections, bug fixes, release notes, upgrades and changes to the Service and Documentation, as developed by Gabi and made generally available for Production use without a separate charge to Customers.

"Intellectual Property Rights" means any and all common law, statutory and other industrial property rights and intellectual property rights, including copyrights, trademarks, trade secrets, patents and other proprietary rights issued, honored or enforceable under any applicable Laws anywhere in the world, and all moral rights related thereto.

"Law" means any local, state, national and/or foreign law, treaties, and/or regulations applicable to a respective party.

"Malicious Code" means viruses, worms, time bombs, Trojan horses and other malicious code, files, scripts, agents or programs.

"Order Form" means the separate ordering documents under which Customer modifies or enhances the Gabi Service pursuant to this Agreement that have been fully executed by the parties.

"Open Source Software" shall have the meaning set forth in Section 3.4 of this Agreement.

"PII" or "Personally Identifiable Information" means any information provided by Customer to Gabi or Gabi Voice relating to an identified or identifiable individual, including, but not limited to, social security number or other unique identifier, health or medical information, credit or debit card numbers, bank account numbers or other financial information, driver's license numbers, and other types of sensitive personal information.

"Product" means the Service and related Hardware that allows persons with disabilities to better access a multifunction printer, the Gabi SmartBox that controls the printer/copier and communicates with our cognitive intelligence engine.

"Security Incident" shall have the meaning set forth in Section 5.3 of this Agreement.

"Software as a Service" or "SaaS" or "Service" mean software-based AI and voice-enabled services (collecting, processing, manipulating, transmitting and storing data) provided to Customers by means of a software application or applications hosted remotely by or on behalf of Gabi and further described in the Gabi Subscription Services Agreement to be executed by Customers.

"SLA" means the Gabi Support and Service Level Availability Policy at Exhibit A, which may be updated by Gabi from time to time.

"Subcontractor" means an entity engaged by Gabi to fulfill part or all of its obligations specific to this Agreement and not suppliers or vendors Gabi may engage in general to provide the Service for its general customer population in a manner that is not specific to this Agreement.

"Term" has the meaning set forth in Section 9.1.



gabi | voice

Your Xerox® Voice Recognition Solution

In a commitment to be the vendor of choice for consumers seeking product accessibility, Xerox® and Gabi® Solutions have formed a strategic partnership in support of a 508c solution for your Xerox® Multifunction Printer (MFP).

Powered by IBM Watson®, Gabi Voice allows workers with physical, mental, and learning disabilities within today's workforce to interact with their Xerox® MFP. By using the wake-up word *Hey Gabi*, you can now tell your Xerox® device to make a copy, send an email, fax, and even access secure print functionalities on the device.

Want to learn more?

Why Gabi Voice?

From Social Security Numbers to Credit Card information, the data you run through your Xerox® Multifunction Printer can be extremely sensitive.



Your jobs issued through Gabi Voice are interpreted securely and accurately at all times. Your data is not stored or transmitted to a third party by neither Gabi Solutions nor IBM Watson®.

Gabi Voice complies with Federal 508c compliance terms enabling the visually impaired and those with learning disabilities to use the MFP's features via natural language.



Disabled workers can now vocalize voice commands through Gabi and watch their MFP execute them flawlessly whether it be making a copy, checking your toner levels, and send an E-Mail.

Getting Started with Gabi Voice – What's Included?

When unboxing your Gabi Voice package, you'll receive the following components:

1-to-1 Gabi Smartbox: An Ethernet/USB equipped micro-controller device designed to communicate directly with the MFP.

Speaker: An on-site microphone/speaker that aids the user in communicating vocally with Gabi. This device connects directly to the Gabi Smartbox via USB.

Power: 5.1v micro USB power adapter UL approved to power up your Gabi Smartbox at all times.

To learn more about Gabi Voice, visit www.gabisolutions.com/gabi-voice



300 John Street
Greer, SC 29651



Call (888) 414-GABI (4224)



Support@GabiSolutions.com

Xerox® Workplace Suite 5.4

Security Guide



© 2019 Xerox® Corporation. All rights reserved. Xerox®, AltaLink®, VersaLink®, Xerox Extensible Interface Platform® are trademarks of Xerox® Corporation in the United States and/or other countries. BR27653

Apache OpenOffice™ is a trademark of the Apache Software Foundation in the United States and/or other countries.

Apple® and Mac® are trademarks of Apple, Inc. registered in the United States and/or other countries.

Chrome™ is a trademark of Google Inc.

Firefox® is a registered trademark of Mozilla Corporation.

Intel® Core™ is a trademark of the Intel Corporation in the United States and/or other countries.

IOS® is a trademark or registered trademark of Cisco in the United States and other countries and is used under license.

Microsoft®, SQL Server®, Microsoft®.NET, Windows®, Windows Server®, Windows 7®,

Windows 8®, Office®, Excel® and Internet Explorer® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Xerox® PDF Reader Powered by Foxit Software Company (<http://www.foxitsoftware.com>).

This product includes software developed by Aspose (<http://www.aspose.com>). Document Version: 1.0

BR27653

Other company trademarks are also acknowledged.

Document Version: 1.0 (October 2019).

Copyright protection claimed includes all forms and matters of copyrightable material and information now allowed by statutory or judicial law or hereinafter granted including without limitation, material generated from the software programs which are displayed on the screen, such as icons, screen displays, looks, etc.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Table of Contents

1. Introduction	1-1
Purpose	1-1
Target Audience	1-1
Disclaimer	1-1
2. Product Description	2-1
Overview	2-1
Print Management Workflow	2-1
Authentication.....	2-1
Single Sign-On	2-1
Desktop Printing	2-2
Mobile Print Workflow	2-2
Submission Methods	2-3
Release Methods	2-3
Combined Submission / Release Methods	2-3
Content Security Workflow.....	2-3
Diagrams	2-4
Simple Workplace Suite Components	2-4
Advanced Workplace Suite Architecture.....	2-4
Single Sign-On Components.....	2-6
Description of System Components.....	2-6
3. System Architecture	3-1
Xerox® Workplace Suite Server	3-1
Xerox® Workplace Suite Volatile Memory	3-1
Xerox® Workplace Suite Non-Volatile Memory	3-1
Print Server Running Job Agent Service	3-1
Print Server and Job Agent Service Volatile Memory	3-2
Print Server and Job Agent Service Non-Volatile Memory	3-2
Document Conversion Engine	3-2
Document Conversion Engine Volatile Memory	3-2
Document Conversion Engine Non-Volatile Memory.....	3-2

Client PC Running Job Agent Client	3-3
Client PC and Job Agent Client Volatile Memory.....	3-3
Client PC and Job Agent Client Non-Volatile Memory.....	3-3
Open Source Components	3-3
4. System Interaction	4-4
Xerox® Workplace Suite Server	4-4
Administration Services.....	4-4
User Portal Services	4-5
Mobile Print Workflow Details	4-5
Print Management Workflow Details.....	4-5
Rules Processing	4-6
Content Security Processing.....	4-6
Copy and Scan Job Processing.....	4-6
Single Sign-On	4-7
Xerox® Workplace App (formerly Print Portal)	4-7
Xerox Managed Cloud Based Routing Service	4-8
Document Conversion Servers	4-8
Document Storage	4-9
Job Agent Service / Workplace Client.....	4-9
Job Agent Service	4-9
Workplace Client	4-10
Document Storage	4-10
Mobile Print Workflow	4-10
Print Management Workflow.....	4-10
Xerox® Workplace Suite Database	4-11
LDAP / ADS Server.....	4-11
LDAP Authentication	4-11
LDAP Import.....	4-11
Printer.....	4-12
Secure Print.....	4-12
Printer Authentication.....	4-12
Xerox® Workplace Suite: Printer Client App	4-13
Xerox Apeos.....	4-13
Customer Email Server(s).....	4-13

Network Appliance	4-14
Xerox® Services Manager	4-14
Export Jobs to Xerox® Services Manager	4-14
Import Printers / Sites from Xerox® Services Manager	4-15
App in the Gallery	4-16
App Server	4-16
User and Email Server Communication	4-16
Xerox® Workplace App and Xerox® Workplace Suite Service	4-17
Customer Email Server and Xerox® Workplace Suite Service Communication	4-18
Workplace Suite Server and Printer Communication	4-19
Discovery	4-19
Printer Client (EIP App)	4-19
Print Authentication	4-19
Scan and Copy	4-19
Administrator Configuration and the Workplace Suite Server	4-20
Document Conversion Server and Workplace Suite Service Communication	4-20
Document Conversion Server and the Printer	4-20
User Workstation and Print Server Communication	4-21
Job Agent Service/Client and Xerox® Workplace Suite Server Communication	4-21
Job Agent Service Start Up	4-21
Job Agent Client Configuration	4-21
Job Management	4-21
Primary Print Server and Secondary Print Server	4-22
Job Agent Service and Printer Communication	4-22
External Communication Between Xerox® Workplace Suite Service and Xerox® Cloud Services	4-22
Xerox® Services Manager and the Windows Azure Service Bus	4-22
Mobile Devices and the Windows Azure Service Bus	4-22
Mobile Devices and the Managed Cloud Based Routing Service	4-23
Xerox® Workplace Suite and LDAP / Active Directory Communication	4-23
LDAP / Active Directory Authentication	4-23
Active Directory Import	4-23
Active Directory On-Boarding Using Email	4-23
Communication Between Xerox® Workplace Suite and Xerox® Service Manager	4-24

Communication Between Xerox® Workplace Suite and Workplace Suite Reporting Service in Azure	4-24
Communication Between the App from the Gallery, the App Server, and the Xerox® Workplace Suite Server	4-25
5. Logical Access, Network Protocol Information.....	5-1
Protocols and Ports.....	5-1
Xerox® Workplace App Ports	5-1
Xerox® Workplace Suite Ports	5-1
Document Conversion Engine Server Ports	5-6
Print Server Ports	5-6
Printer and Printer Client (EIP App) Ports.....	5-7
Job Agent Service Ports.....	5-7
Job Agent Client Ports	5-7
Network Appliance Ports	5-8
iOS Native Printing Ports	5-8
Port Diagram	5-9
Network Port Diagram	5-9
6. System Access.....	6-1
Xerox® Workplace Suite (Web Administration Portal)	6-1
Xerox® Workplace App (Print Portal)	6-1
Workplace Client	6-2
Printer Client (EIP App).....	6-2
User Portal	6-2
7. Additional Security Items.....	7-1
Auto Release via Network Appliance Workflow	7-1
Models	7-1
Audit Log	7-1
DMZ Configuration	7-2
DMZ Setup	7-2
Mobile Devices and the DMZ Server	7-2
Debug Logs.....	7-3
Workplace Suite Server Windows File Structure	7-3
Smartcard (CAC/PIV) Integration.....	7-3
Printer Client Release Permissions	7-3
Administration Recovery	7-4
Single Sign-On	7-4

8. Additional Information and Resources	8-1
Security @ Xerox	8-1
Responses to Known Vulnerabilities.....	8-1
Additional Resources	8-1

1. Introduction

Xerox® Workplace Suite (WS) is a workflow solution that connects a corporation mobile workforce to new productive ways of printing, and controls user access to Xerox® Multifunction Printers (MFP). Printing is easy and convenient from any mobile device without needing standard drivers and cables. This solution also supports Desktop Printing, allowing printing to a common queue with the ability to release jobs to any printer. This reduces waste from uncollected jobs and provides security for sensitive information, since jobs are only printed when the user is standing at the printer.

WS has been extended in version 5.0, providing a single sign-on (SSO) infrastructure. Apps in the Xerox App Gallery which have been modified to support this new infrastructure may use WS as a storage vault for user login information (e.g., credentials or tokens). After logging into WS, a user may select an SSO enabled Gallery App, which queries WS to obtain the user's login information for that app. If available (and valid...e.g., not expired), the app uses that information to log the user into the Gallery App without the need to provide additional login credentials.

Purpose

The purpose of the Security Guide is to disclose information for Xerox® Workplace Suite with respect to application security. Application security, in this context, is defined as how data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. This document describes design, functions, and features of the Xerox® Workplace Suite relative to Information Assurance (IA) and the protection of customer sensitive information. Please note that the customer is responsible for the security of their network and the Xerox® Workplace Suite does not establish security for any network environment.

This document does not provide tutorial level information about security, connectivity or Xerox® Workplace Suite features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security. It is assumed that the reader is familiar with the solution; as such, some user actions are not described in detail.

Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Product Description

Overview

The Xerox® Workplace Suite provides three primary workflows:

- Print Management Workflow (which includes Single Sign-On for supported Gallery Apps)
- Mobile Print Workflow
- Content Security Workflow

Print Management Workflow

There are two parts to the Print Management workflow: Printer Authentication and Desktop Printing and Release.

Authentication

Defined as customers who require validation of user access to MFPs before device usage is allowed at the “All Services” screen. Card-based is the most widely used authentication method. User name and PIN-based login at the device is an alternate method of login when card readers are not installed or are not functional. Authentication as a standalone option provides device security access only, for the customer who does not require print jobs associated with their network login. Supported authentication mechanisms include:

- Cards (e.g., HID Prox)
- Alternate Login
 - Email and Confirmation Number
 - PIN (card number)
 - LDAP/AD
- Mobile Phone Unlock using the Xerox® Workplace App: supporting NFC, QR Codes and Unlock Code Entry
- NFC Unlock with a support USB Card Reader (Android Only using Elatec TWN4 Reader with NFC unique programming)

Single Sign-On

Xerox and its partners offer different types of Apps in the Xerox App Gallery, many of which require some type of user authentication. These Apps typically requiring unique login credentials for each one. In order to improve this user experience, WS offers a Single Sign-On (SSO) capability, where users log into the printer, and are then able to select one of these supporting Gallery Apps without the need to provide additional credentials.

The Single Sign-On feature allows WS to store user access information for Xerox® Gallery Apps that have been designed to support the single sign-on feature. The Authentication solution now becomes an SSO vault. The SSO vault acts as a storage vault, where login information for each supported/enabled Gallery App is stored.

As an analogy, you can think of the SSO vault (e.g., XWC) as a security vault with a collection of safety deposit boxes. Each user is given a safety deposit box that is unique for that user and a specific App (e.g., the File and Print Dropbox App). To access the safety deposit box, the user provides their identity (i.e. they log into the printer) and then indicates which safety deposit box they wish to access by selecting an App on the User Interface of the printer. The App then views the contents of the safety deposit box from the security vault or they may update or delete the contents.

All content to be stored in the vault is encrypted by the App (or its backend hosted system) before being given to the SSO vault. This ensures that the SSO vault can never view or use the contents being stored in the vault. Only the App infrastructure knows how to decrypt and use the contents of the vault.

Desktop Printing

The Workplace Suite supports the Desktop Print feature using two different print queue types.

1. Network Queues – where jobs are printed to a shared Windows network print queue and can then be routed or processed appropriately according to the print workflow (Direct or Pull-Print).
2. Client Queues – where jobs are retained locally on the user's client PC until they are routed and processed, again based on the print workflow (Direct or Pull-Print). This method requires the installation of a desktop client on the user's workstation.

For either of the above print server models, the administrator may configure the type of print workflow that they would like to use. The two supported workflows:

1. Pull Print – where jobs are held until the user authenticates themselves at a printer and releases.
2. Direct Print – where jobs are sent immediately to the printer that is associated with the queue.

Rules and Quotas can also be applied to desktop jobs, which allows control over who is able to print, to which devices and at what time as well as controlling how many pages can be printed. Rules can also be used to control which print features (color or 2-sided) are available to users.

Mobile Print Workflow

The workflow of mobile printing is quite simple. A user using a mobile device such as a smart phone, tablet, or laptop sends a document to the Xerox® Workplace Suite. Depending on the submission method, the job is either printed without any further user action or the user manually releases the job to print. Rules can also be applied to mobile print jobs, which allow control over who is able to print, to which devices and at what time. Rules can also be used to control which print features (color or 2-sided) are available to users.

There are several methods for a mobile user to submit or release a job to print. The Submission method is technically decoupled from the release method. However, certain submission/release pairs make more sense than other pairs.

Submission Methods

- E-mail
- Xerox® Workplace App (formerly Print Portal)
- Simple Desktop Print Service (upload)

Release Methods

- Printing device UI (via EIP)
- Xerox® Workplace App (formerly Print Portal)

Combined Submission / Release Methods

(Note: jobs print without any explicit user action after submission):

- E-mail
- Xerox® Workplace App (formerly Print Portal)

Content Security Workflow

The Content Security Workflow allows an administrator to create Content Profiles and define search strings which are used to track documents processed by WS. The administrator can define actions that will be taken when a document is searched and found to match a Content Profile. The possible actions include:

- Logging the matching Content Profile name in the Job History.
- Emailing (notifying) a list of recipients with details on the job (e.g., who printed it, name of the job, the device it was printed to, the time and date it was printed and the matching Content Profile name.
- Storing a copy of the job for audit purposes.

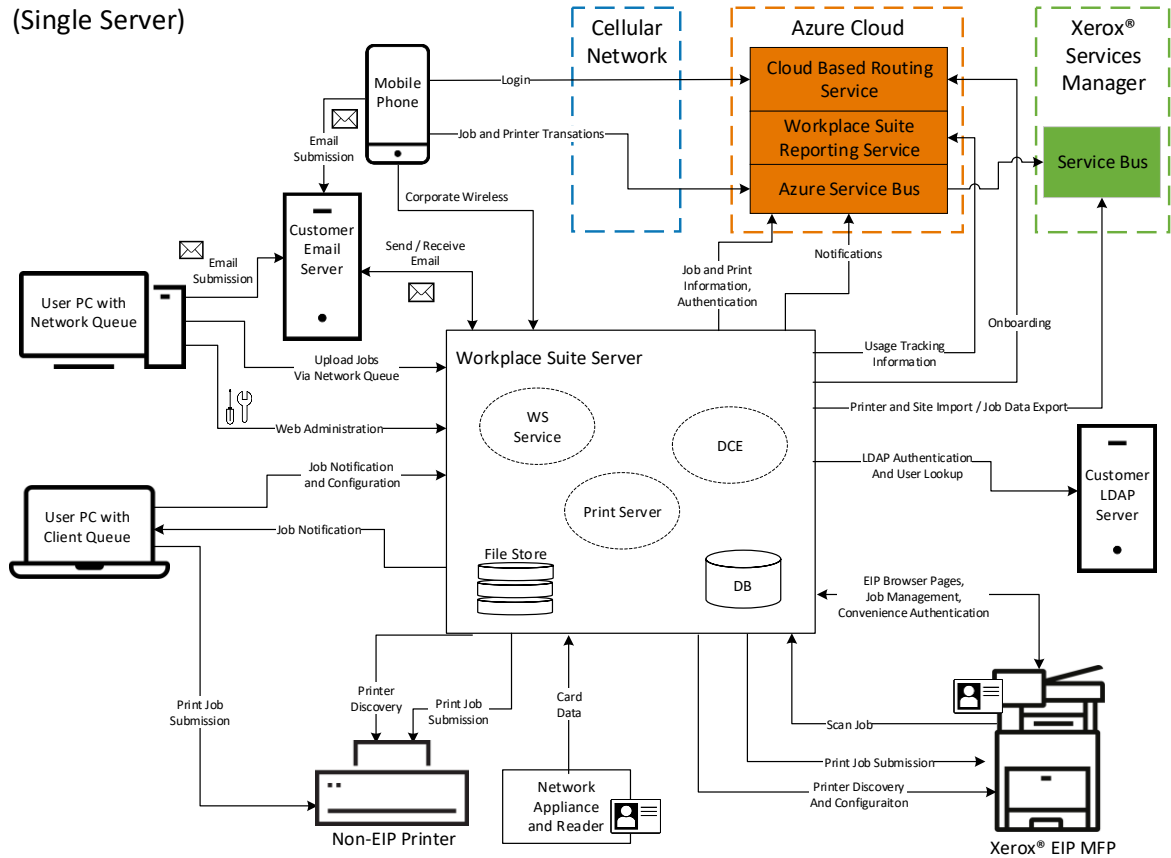
Diagrams

The below diagram shows a couple of example system component / architecture diagrams for different sized customers using the Workplace Suite for both the Print Management and Mobile Print Workflows. These diagrams and their components will be discussed in greater detail in the following sections of this document.

Simple Workplace Suite Components

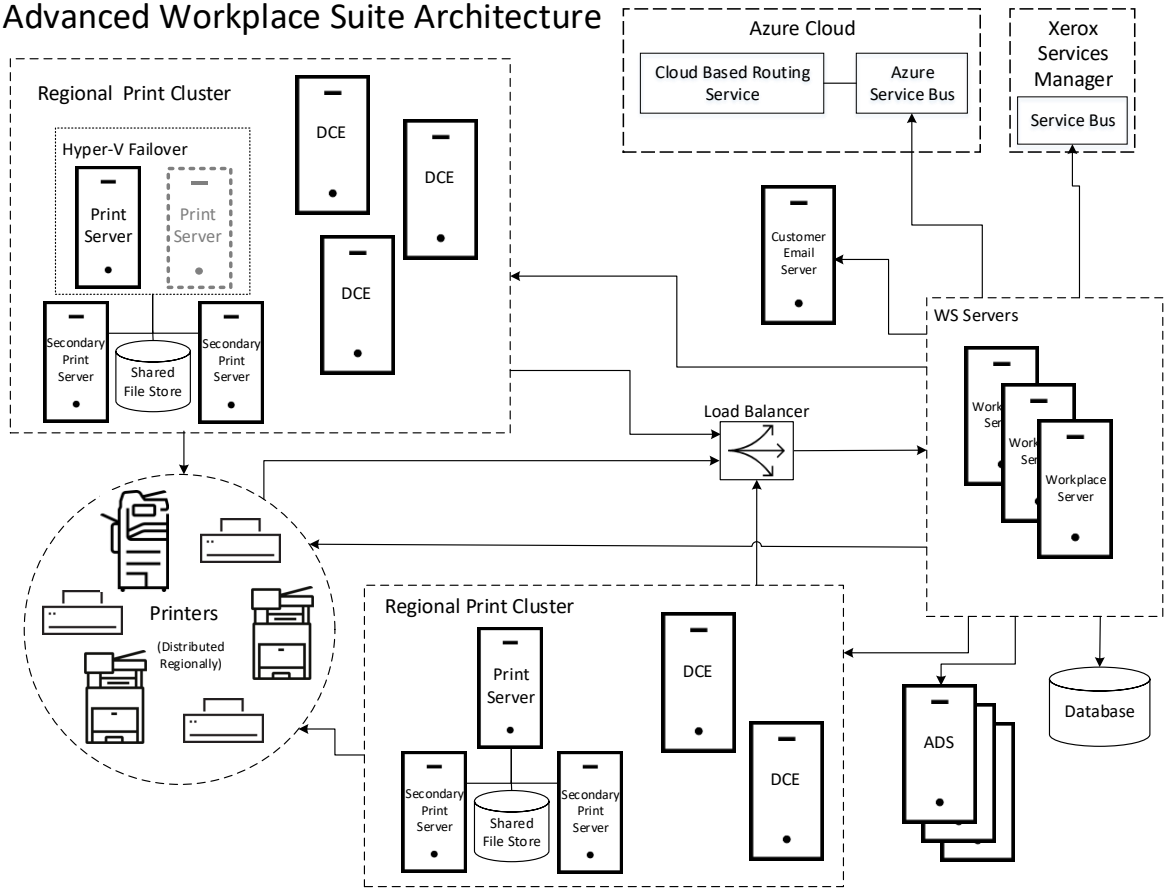
Simple Workplace Suite Architecture

(Single Server)

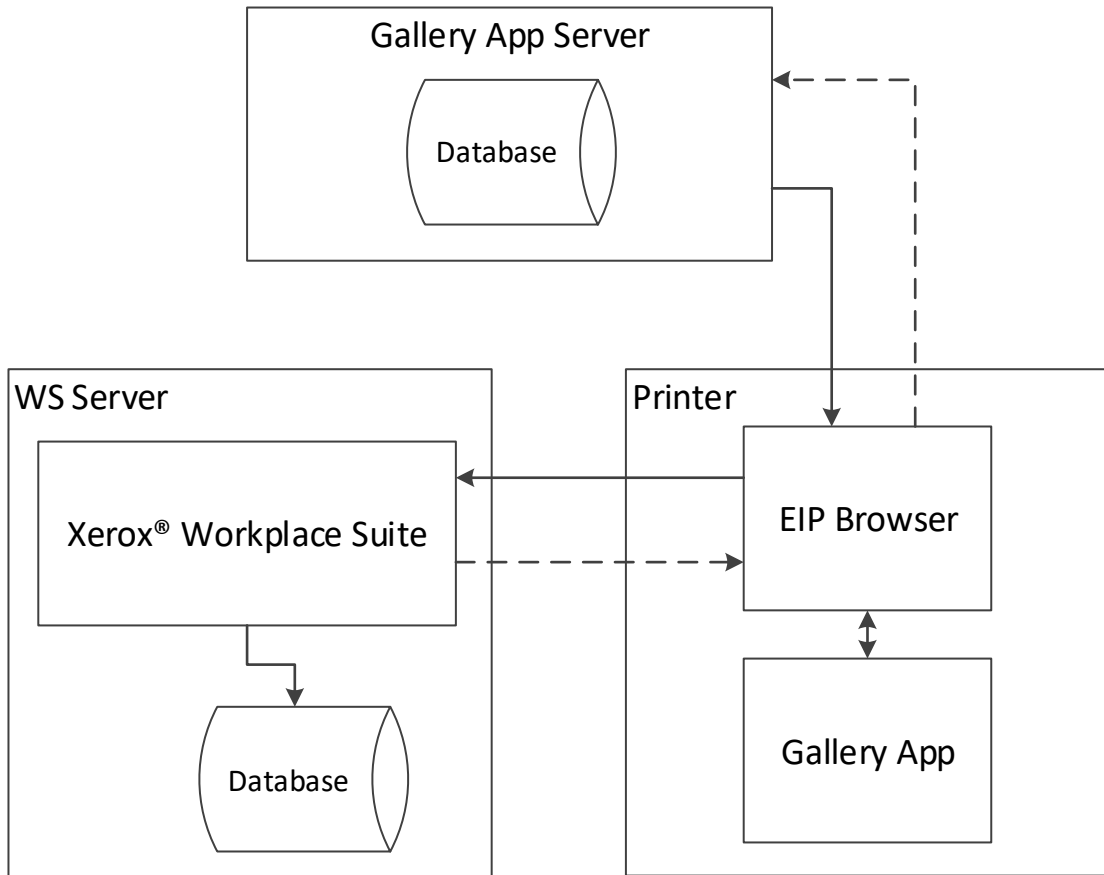


Advanced Workplace Suite Architecture

Advanced Workplace Suite Architecture



Single Sign-On Components



Description of System Components

Component	Description
User	A user of the WS system.
Xerox® Workplace Suite	On premise application that runs on customer provided hardware/server, which supports Printer Discovery, Printer Management, Print Routing, EIP Web Page Host, Administration Host, and Convenience Authentication.
Xerox® Workplace App (print portal)	Mobile Phone application that allows the user to find printers and upload / send print jobs to WS.
Xerox Cloud Services	Xerox Cloud Services hosted on Microsoft Azure that support Mobile Phone authentication, printer discovery and print submission.
Customer ADS/LDAP Server	Used for user authentication.
Print Server with Network Queues	Windows PC hosting Shared Network Print Queues running the Job Agent Service. Handles job routing, notifying the WS of new jobs, parses jobs, modifies job for selected attributes, and transmits jobs to the printer on release.
Document Conversion Engine (DCE)	Converts mobile jobs to print ready format upon release and transmits jobs to the printer.

Component	Description
SQL Database	Storage of WS configuration, user info, job info, job history.
File Storage	Storage of print jobs.
Printer	Any printing device (Xerox® or Non-Xerox®) that is enabled to support WS.
Customer Email Server	The Customer Email Server is used to get print jobs to the Xerox® Workplace Suite.
User PC with Network Queue and/or Client Queue	User's system on which network print queues or client queues (using the desktop client) are installed.
Network Appliance	External hardware device that supports card-based document release at Non-Xerox or Non-EIP Devices.
Xerox® Services Manager	External Xerox application used in managed service accounts.
Workplace Suite Reporting Service	Collects usage information used to improve future performance and functionality of the solution.
App from App Gallery	An App found in the Xerox App Gallery that has been modified to support SSO.
App Server	A backend system that handles the browser-based calls and processing needed by the App. Maintains knowledge and information about the SSO server.

3. System Architecture

Xerox® Workplace Suite Server

The Xerox Workplace Suite server is the primary server for this Xerox solution. It is responsible for handling administration and configuration of the system, orchestration of all components and services, performing authentication and serving EIP browser pages, performing usage tracking and job management. WS runs on a Windows based server or PC.

Xerox® Workplace Suite Volatile Memory

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
RAM	Varies based on customer system	N	Executable code, temporary storage for messages processing related data, variables, state information, etc.	Y	Power Off or Exit of the Service

Xerox® Workplace Suite Non-Volatile Memory

Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
HDD	Varies Based on Customer System	Y	Storage of binaries, libraries, graphic images, HTML pages, JavaScript pages, certs, configuration, logs, user documents, print drivers, installers, templates, job metadata	Y	Requires uninstall of software and then manual removal of remaining files (e.g., logs and database file)

Print Server Running Job Agent Service

Print Servers for WS are Windows Servers running the Job Agent Service (JAS). Print Server can run as standalone systems, separate from the WS main server, or the JAS can run on the same system as the WS server software. The Print Server / JAS is responsible for accepting incoming jobs, storing them to the designated location, parsing jobs to detect user and accounting information as well as job attributes, notifying the WS system of the job, updating job attributes and transmitting released jobs to the printer.

Print Server and Job Agent Service Volatile Memory

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
RAM	Varies Based on Customer System	N	Executable code, temporary storage for processing related data, variables, state information, etc.	Y	Power Off or Exit of the Service

Print Server and Job Agent Service Non-Volatile Memory

Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
HDD	Varies Based on Customer System	Y	Storage job and related info, configuration, logs.	Y	Removal / Un-install of the JAC. Manual removal of some files after uninstall is required (e.g., job information).

Document Conversion Engine

Document Conversion Engine Volatile Memory

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
RAM	Varies Based on Customer System	N	Executable code, temporary storage for processing related data, variables, state information, etc.	Y	Power Off or Exit of the Service

Document Conversion Engine Non-Volatile Memory

Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
HDD	Varies Based on Customer System	N	Storage of binaries, libraries, logs, printer information, print job data.	Y	Removal / Un-install of the DCE. Manual removal of some files after uninstall is required (e.g., job information).

Client PC Running Job Agent Client

Client PC and Job Agent Client Volatile Memory

Type (SRAM, DRAM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
RAM	Varies Based on Customer System	N	Executable code, temporary storage for processing related data, variables, state information, etc.	Y	Power Off

Client PC and Job Agent Client Non-Volatile Memory

Type (Flash, EEPROM, etc.)	Size	User Modifiable (Y/N)	Function or Use	Contains Customer Data	Process to Clear:
HDD / SSD	Varies Based on Customer System	N	Storage of binaries, libraries, printer information, print job data	Y	Removal / Uninstall of the DCE. Manual removal of some files after uninstall is required (e.g., job information).

Open Source Components

Xerox® Workplace Suite does make use of Open Source software modules in its different components (e.g., the Workplace Suite Server, DCE, JAS/JAC, etc.). An up to date bill of materials for this solution is available upon request from Xerox.

4. System Interaction

This section describes the system components and their interfaces.

Xerox® Workplace Suite Server

The Workplace Suite server is the foundational component of the Xerox® Workplace Suite solution, used to manage the system's behavior and user's interaction within the system from authentication, document submission, and printing. The Xerox® Workplace Suite Server (WSS) is a Windows® application running on a Windows® Server. WSS will conform to the customer's existing security policies, using Windows® based authentication to access this application. It is recommended that access to the server be limited to Systems Administrators and authorized Xerox® personnel.

Users authenticate themselves at a printer using the WSS. In addition, user's documents are received and either stored for secure release or directly printed at a printer. The Xerox® Workplace Suite server monitors and works in conjunction with the available Conversion Servers for document conversion and print processing, as well as the Job Agent Clients and Print Servers on receiving and releasing desktop print jobs. The XWSS provides Single Sign-On functionality for supported Gallery Apps.

For network communication using HTTPS, the WSS supports TLS versions 1.0, 1.1 and 1.2. Support for SSL v2/v3 has been deprecated.

There are a number of sub-functions of the Xerox® Workplace Suite server, which are discussed in greater details below.

Administration Services

The WSS administration services provide configuration, user, printer and job management.

The administrator interacts with the Administration Services via a web browser interface to perform tasks such as creating an incoming email account to receive jobs upon, managing users, registering printers, and enabling features. Connection to the Administration Services is supported via HTTP (port 80) or HTTPS (port 443). By default, the Workplace Suite Server uses a self-signed certificate for HTTPS communication.

[Please note that most web browsers will generate a warning when using the self-signed certificate as it was not generated by a trusted authority].

The administrator has the option to load and use a certificate from a trusted certificate authority on the Xerox® Workplace Suite server.

The Workplace Suite Admin webpage is accessed via a web browser. By default, the system uses an email address and confirmation number to access the administration interface the first time. From there, the administrator may select the desired authentication mechanism for both web administration and user portal (see next section) access. The supported authentication mechanisms are:

- Email and Confirmation Number – User can login using their email and a system generated Confirmation Number.
- LDAP Authentication – User can login using their LDAP credentials. At least one LDAP Connection must be enabled to select this option.

- Windows Integrated Authentication - When this option is enabled, users will not be required to log into the User Portal. Workplace Suite will use the identity of the current Microsoft Windows session to log the user into the portal.

User Portal Services

The WSS User Portal provides the ability for a user to manage settings and configuration specific to themselves. At this time, this is limited to being able to view and manage Release Permissions for the Printer Client (EIP App). Refer to section “7.5 – Printer Client Release Permissions” for further details on this feature.

Users interact with the User Portal via a web browser interface. Connection to the User Portal is supported via HTTPS (port 443). By default, the Workplace Suite Server uses a self-signed certificate for HTTPS communication.

Mobile Print Workflow Details

By default, the Mobile Print Workflow allows any user to create an account within the system. Accounts are created whenever an email submission is received or when the Xerox® Workplace App (print portal) is first used to access the system.

However, the system can be configured to only allow a specific set of users (an allowed-list) or to not allow a specific set of users (a block-list).

When an account is created the user receives a system generated confirmation code. The confirmation code is used to access their jobs at the MFP or to connect the Workplace App to the server.

All users' jobs are stored and referenced based upon the user's email address. User's jobs are stored in the Workplace Suite Server Windows file system with a randomized file name. By default, they are not encrypted, however, an Encrypted File System (EFS) may be configured manually.

Unprinted jobs are deleted based upon an administrator configured retention period. The default retention period is 1 day. The Retention Settings apply to Third Party Print Queues in addition to printers. Sending documents to a Third-Party Print Queue is equivalent to the print command in the Mobile Print Workflow. This means that if the system is configured to delete documents after printing, documents are deleted after sending them to a print queue. Based on this same example, if a default print queue is set on the system, all emails sent to Workplace Suite are in turn sent to the default print queue and immediately deleted from the system.

Print Management Workflow Details

By default, the Print Management Workflow supports auto-registration. If the customer site uses LDAP or Domain controllers, then auto-registration allows the user to scan their badge (or Android phone with NFC) via a connected USB card reader at a Print Management (authentication) enabled printer. The user would then provide their LDAP authentication credentials to validate their identity, resulting in the addition of that user and their relevant LDAP information (name, email, network user name) in the Workplace Suite user database. The solution can support multiple badges per user if desired. If auto-registration is not used, there are other options to create and manage users, including: Manual Updates, CSV Import, and LDAP Import.

All submitted jobs are stored and referenced based on the user's network user name and email address. The user's jobs are stored in the print server's Windows file system, or on the client with a randomized file name.

Unprinted jobs are deleted based on an administrator configured retention period. The default retention period is one day.

Rules Processing

The WS system allows the administrator to define rules which are applied at print release time (applies to copy jobs as well). There are 2 types of Rules available in WS.

1. Print Controls – are used to determine which printers are available, the time and day when they can be accessed and what attributes may be used when processing jobs for any given user.
2. Print Quotas – are used to set a page limit per user that they are allowed to print during a given time period (daily, weekly, monthly).

By default, no rules are defined. Users may access any printer, at any time, and all print attributes are available. In addition, there are no print quotas defined, so users can print an unlimited number of pages. When one or more rules have been defined and enabled, the system switches to a permission access mode. In order to print, the user must be granted permission to print to a given device using a rule. The administrator can control which devices, which time of day and which attributes are available to the users of the system. If there are no rules allowing a user to print, based on the device being used and the time of day, then the user's job is blocked from printing after release.

If a user exists in multiple rules, then all rules are checked at the time of print release. If there is at least one rule allowing the user to print to the given device based on the time of day, then the jobs are allowed to complete. If there are multiple rules that map the current printer and time of day, which have conflicting print feature access (e.g., color and single-sided), the rule(s) granting access to these features take precedence).

Rule processing always occurs on the WS server. This processing determines if a user is allowed to release a print job on a given printer, at the current time and if any job attributes need to be modified (e.g., change to black & white or duplex). The actual job attribute changes occur in different components based on the location of the job: JAS/JAC for desktop jobs and the DCE for mobile jobs.

Content Security Processing

The processing of jobs for Content Security occurs at the time the job is uploaded into the WS system. This implies that the processing occurs in different components based on entry into the solution. For desktop submitted jobs using the Print Management Workflow, the JAS/JAC components handle content security processing. For Mobile Print jobs and Copy and Scan jobs, the WS server handles the processing. The WS server handles the coordination of the results of the content security processing and ensuring the configured options for a matching profile is applied: Logging, Email Notification and Storing.

In the case of Content Storing of a job, the administrator defines the location of where the data will be stored using the web admin as well as the retention period of the stored files. The maximum allowed retention period is one year. Once the retention period is reached, the stored file(s) are deleted. As with any Microsoft server OS, the deleted documents follow traditional Microsoft Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Workplace Suite provides no facilities to erase the documents themselves. The stored files are not encrypted by WS. However, file Encryption is available using the Microsoft built-in Encrypted File System (EFS) feature.

Copy and Scan Job Processing

The WS solution supports the ability to perform Scan and Copy jobs. Both job types result in the scan job being sent or pulled to the server. The job is stored temporarily in the Content Partition Storage location until it is printed or emailed. The job is deleted after it is transferred to the final destination. If Content Security is enabled and the job matches a Content Profile that is configured

with the content storage option, the original PDF received from the scan is then stored in the configured content storage location. If Rules are enabled, then they are applied to Copy jobs, as copies result in printed / marked pages.

Single Sign-On

The WS Server provides the SSO functionality that can be called or access from supported Apps in the Gallery. The server acts as the network interface accepting and responding to requests to store or retrieve authentication information as well as the keeper of that information. All SSO related information is stored in the SQL database used by WS. Sensitive information such as the actual stored authentication data, the private key used to decrypt the SSO requests sent by an App and the public key used to validate signed requests from an App are all stored in encrypted format (SHA256) within the SQL database.

Xerox® Workplace App (formerly Print Portal)

The application uses a Xerox managed cloud-based routing service to direct the user to the appropriate Xerox® Workplace Suite server. Once authenticated, the user's credentials and authentication token are stored in the application until they log out.

The Workplace Suite Admin has control over how often a user will need to re-supply their credentials when using the Workplace App. An option exists to retain the logged-on user's credentials within the app, such that any subsequent logon will not require the user to re-supply their credentials. The Admin may also control the length of time that the user will remain logged into the account when using the Workplace App. Users will be required to re-supply their credentials once the once the timeout is reached. If the Admin has enabled the "Retain Login Credentials" feature, then the user would automatically be logged back into the system after the expiration time period.

Users can only access jobs that they have submitted. This includes Print Management Workflow (Pull-Print) jobs as well. With the Workplace App, users can preview their jobs, see a list of available printers, select print options and submit their job for printing.

For security reasons, enabling and accessing the Workplace Suite server using the Workplace App is a multi-step process:

1. An administrator must enable the use of the Workplace App via Administration Services at the Workplace Suite Server, the result of which is a "company code." The Workplace Suite administrator must distribute this code to authorized users. [Note: An administrator may request a new company code at any time.]
2. During initial log-in a user must enter their email address and company code.
3. The Workplace Suite system generates a confirmation code and sends the confirmation number to the user at the supplied email address.
4. The user must then enter the confirmation code into the Workplace App.

The Mobile Print Workflow supports both an allowed-list and a block-list capability. An allowed-list would restrict access to only a specified set of user email addresses; a block-list would disallow these email accounts.

Lastly, if a user needs to reconfigure the Workplace App from one company code to another, an action verification code is sent to the user by the Xerox® Workplace Cloud (Cloud Hosted) itself.

For customers that have installed both the Mobile Print Workflow and the Print Management Workflow, the Workplace App supports the ability to authenticate with an enabled printer. There is an option in the menu of the app called "Unlock Printer". This option allows you to use your phone

to authenticate with a device in place of a card or using Alternate Login. The supported logon methods for mobile phone unlock include:

- NFC (Android and iOS, where your iOS device must be an iPhone 7 or newer running iOS 11 or later). [Feature requires a Xerox® VersaLink or Xerox® AltaLink series printer]
- QR Code – You may scan the QR code found on the welcome page or on the blocking screen of the printer user interface panel.
- Unlock Code – You may enter the 4-character code found on the authentication blocking screen of the printer.

The Workplace App supports iOS native printing. This print mechanism uses a combination of printer discovery, via either mDNS or DNS-SD to locate a compatible printer. If using mDNS, the Apple Bonjour Service must be installed on the Xerox® Workplace Suite server, and the standard Bonjour ports must be opened on the server's firewall. The Xerox® Workplace Suite Server responds to mDNS queries and advertises itself as a printer, thereby allowing Workplace App users to submit print jobs to Workplace Suite using iOS native printing. Alternatively, the IT administration at a customer site can configure their DNS servers to advertise the Xerox® Workplace Suite server as a printer. This allows client applications such as Workplace App to use DNS-SD (service discovery), to discover the Workplace Suite Server as a printer. Regardless of the type of discovery method, once found, the Workplace App can submit (upload) jobs to the Xerox® Workplace Suite server using IPP (port 631). Jobs are then available for release using the Workplace App to a printer, or the Printer Client (EIP) Application.

There is a version of the Workplace App that supports Google Chromebooks as well as an extension to the Google Chrome browser. When run in these environments, the Workplace App supports “single sign-on” using your Google credentials to validate the user in place of manually entering credentials.

Xerox Managed Cloud Based Routing Service

The managed cloud routing service provides a “routing” capability between the Workplace App, running on a customer's smart device, and the Workplace Suite Server running within the customer's network. Messages are sent from the Workplace App to the Cloud Service.

The managed cloud-based routing service runs on the Microsoft Windows Azure Platform (see below). All communication is handled using Industry standard HTTPS protocols. The security certificate is issued by Comodo (a trusted certificate authority) and ensures that the application has been verified and validated.

For more information on Windows Azure Security, please visit:

<http://azure.microsoft.com/en-us/support/trust-center/>

Document Conversion Servers

The Xerox® Workplace Suite is modular in design, leveraging a core Workplace Suite server component as well as one or more additional Mobile Print Workflow components referred to as Conversion Servers. The Conversion Server converts documents from their native format (e.g., .doc, .ppt) to a print ready file (e.g., Postscript, PCL) that the destination printer understands. A Conversion Server may reside on the same server as the Xerox® Workplace Suite server, or it may reside on a separate server. Only one Conversion Server may reside on any given server.

Document Storage

Both the native format document and the print ready file are temporarily stored to the Conversion Server system disk while the files are active. Once the Conversion Server has completed the document conversion process, the print ready document is stored in the configured Content Storage location, which could be local to the DCE or a shared network resources (e.g., RAID system). Any temporary files created during the conversion process are deleted from the Conversion Server disk and memory after storing the print ready document.

The print ready file is deleted from the system once the original is deleted.

As with any Microsoft server OS, the deleted documents follow traditional Microsoft Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Workplace Suite provides no facilities to erase the documents themselves. In this sense, the Conversion Server is treated as any other document server within the corporate firewall.

Job Agent Service / Workplace Client

The Print Management Workflow is modular in design, leveraging the core Workplace Suite Server, as well as one or more additional components referred to as the Job Agent Service and the Workplace Client. The Job Agent Service runs on the print server and is included as part of the install of the Xerox® Workplace Suite software. For customers who want to use an external print server, they can install the Job Agent Service on one or more external servers to create a distributed or regional system of print servers. For environments that want to forego a traditional print server, they can instead install the Workplace Client on each user's workstation. The Job Agent Service/Client is also responsible for processing incoming print jobs for Content Security. Jobs are processed to see if they match one of the configured Content Profiles. If a match is found, the agent notifies the WS server. If the matching profile has the content storage option enabled, the agent also creates a PDF of the print job and sends this to the WS server to be stored.

Job Agent Service

The Job Agent Service is a Windows service installed on a print server used in conjunction with the Xerox® Workplace Suite software with the Print Management Workflow license. The service can run on the same server running the Xerox® Workplace Suite, or it can run on one or more external print servers. When installed on an external server, the Job Agent Service starts a listening service and waits for the Workplace Suite Server to enable it to perform job management. The Xerox® Workplace Suite administrator must add the print server IP Address to the list of print servers, effectively enabling the Job Agent Service to begin communicating with the Workplace Suite server. The messaging between the Workplace Suite Server and Workplace Client consists of:

- Reporting of available printers (Queues)
- Enablement of printers (Queues)
- Job Information – Reporting of new jobs and their details
- Notification of job release to an enabled printer
- Results of job transfer to a printer
- Periodic job synchronization

Workplace Client

The Workplace Client is a Windows service installed on a client workstation used in conjunction with Xerox® Workplace Suite Software with the Print Management Workflow license. When installed a user workstation, the Workplace Client must be pointed to the Workplace Suite Server via the inclusion of a configuration file or via a Service Registry setting which can be pushed to the workstation by the customer IT organization. The Workplace Client is responsible for managing print queues and print jobs on the client workstation. The messaging between the Workplace Suite Server and Workplace Client consists of:

- Querying the server for configuration (e.g., polling intervals, timeouts, etc.)
- Querying the server for the list of printers (Queues)
- Installing or removing printers (Queues)
- Job Information – Reporting of new jobs and their details
- Polling or notification for job release to an enabled printer
- Reporting of job transfer to a printer
- Periodic job synchronization

Document Storage

Mobile Print Workflow

Documents are stored unencrypted in the Xerox® Workplace Suite server. The documents are stored in a configurable location†, which can be any location to which the Xerox® Workplace Suite server has access. For performance and configuration reasons, on-box storage is recommended. Access to the documents is protected by Windows and Server access on the client's domain. As a layer of protection, actual documents are stored with an obfuscated file name and extension.

The documents are retained until either:

- The user deletes them via the Print Client App at the device UI or the Workplace App.
- The Xerox® Workplace Suite deletes them after a configurable timeout.

As with any Microsoft server OS, the deleted documents follow traditional Microsoft Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself but are overwritten as the system reclaims the disk space. The Mobile Suite Web Administration UI does provide the ability to delete documents if needed.

Note: Encryption is available using the Microsoft built-in Encrypted File System (EFS) feature.

Workplace Suite limits the maximum size of a submitted file to 1GB or smaller. A utility may be used to modify this value if necessary.

Print Management Workflow

All printers (queues) configured for the Print Management Workflow use the Workplace Suite Port Monitor. Part of the Windows print path, this monitor accepts a print ready file (e.g., Postscript or PCL) and writes it to disk. The location where the file is written is configured using the Workplace Suite Web Admin tool. The print ready file and some descriptor files are temporarily stored on the print server or client workstation system disk while the files are active. Upon release to a printer, the Job Agent Service or Client removes the associated files.

As with any Microsoft server OS, the deleted documents follow traditional MS Windows deletion processes and are deleted from the NTFS list. Documents are not actually deleted from the hard disk itself, but are overwritten as the system reclaims the disk space. The Xerox® Workplace Suite provides no facilities to erase the documents.

Xerox® Workplace Suite Database

Microsoft SQL Express 2014 database is used by Xerox® Workplace Suite as the default relational data store. However, WS can be configured to work with an external Microsoft SQL database. In order to create this database, the user who installs Xerox® Workplace Suite must have permissions to create databases and database logins, and grant permissions. During the installation, Xerox® Workplace Suite grants the system account “Domain\ComputerName\$”, the rights to update the created database.

LDAP / ADS Server

The Xerox® Workplace Suite server retrieves and stores a list of available active directory domains based on the context of the domain to which the WS server belongs. The administrator may also manually add domains if desired. The administrator may then enable or disable domains which can be used for authentication and user import.

LDAP Authentication

The LDAP/ADS Server is part of the customer's network and is not a deliverable of the Xerox® Workplace Suite. Therefore, the security and maintenance of the LDAP/ADS Server is outside of the responsibility of WS.

When the Authentication Type for the Workplace App or the EIP Printer Client App is enabled for LDAP Authentication, or Convenience Authentication is configured for LDAP when using Alternate Login or Auto Enrollment of Cards (or Android phones with NFC and a supported USB card reader), the Workplace Suite Server verifies user credentials against Active Directory. The workplace credentials consist of Domain Name, Domain Username and Domain Password. The Workplace Suite Server performs an LDAP login using the supplied credentials. Passwords are never stored. By default, the system uses SASL when doing an LDAP bind.

In order to communicate with Active Directory, Xerox® Workplace Suite uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems supported by Xerox® Workplace Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used.

LDAP Import

Xerox® Workplace Suite can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP/ADS Authentication. The administrator has the ability to configure the type of LDAP access (Anonymous, Basic, Negotiate) required when connecting the LDAP server. By default, the system is configured to use the Negotiate setting, which instructs the Workplace Suite Server to use SASL when doing an LDAP bind.

The administrator must supply user credentials to be supplied to the LDAP server when performing an import, assuming they have selected either Simple or Negotiate for the Usage Mode. The credentials are stored in the Workplace Suite Server database (SQL), and encrypted using SHA256 and AES.

As part of the import, the administrator can define the LDAP containers that are queried as part of the import and map the fields within those containers to fields within the Workplace Suite user database.

As part of the import, the administrator may configure the type of LDAP records that they wish to import: Additions (new LDAP records), Modifications (updated LDAP records) or Deletions (users that have been removed or marked as deleted in LDAP). As part of the “Deletions” option, the administrator may configure an LDAP Filter specific to each LDAP server to be used when looking for deleted records to be removed from the WS database.

In order to communicate with Active Directory, Xerox® Workplace Suite uses the Active Directory Services Interfaces (ADSI) technology available in all Windows operating systems supported by Xerox® Workplace Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used.

Printer

Xerox printers have a variety of security features that can be employed to increase security. Availability of these features will vary depending on model. It is the customer’s responsibility to understand and implement appropriate controls for printer behavior.

Secure Print

Xerox® Secure Print allows you to control the print timing of your documents. When using Secure Print during print job submission, users enter a passcode, and then must enter the same passcode to retrieve the job at the printer.

Users may choose to use Secure Print with Secure Print enabled printers, or the administrator may configure their system to require that Secure Print be used for all jobs sent via the Mobile Print Workflow to that printer.

Secure Print passcodes are never stored on the mobile App or in the Workplace Suite Server. They are transferred securely over TLS. Passcodes are never stored externally to the job on the printer.

Passcodes are numeric and conform to the requirements of the printer model. Auto-generated passcodes are a minimum of 6 digits for all printers whose maximum is at least 6 digits.

For information on the security of a job while it is stored on the printer, refer to your printer’s documentation.

Printer Authentication

Xerox® multifunction devices introduce a flexible Xerox Extensible Interface Platform® (EIP). This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. Xerox® Workplace Suite uses this platform to secure access to the printer.

Additional security can be enforced at the printer if the printer is EIP capable and/or supports the EIP Convenience Authentication API. For those printers which support this capability, the Xerox® Workplace Suite provides the capability to lock the printer’s local user interface, and require the user to authenticate themselves at the printer in order to gain access to any of the services / features of the printer. There are three ways in which a user can authenticate themselves:

1. The user may supply their Xerox® Workplace Suite user credentials (username / password or LDAP credentials depending upon the Company/Account configuration) at the printer.

2. The user can identify themselves using their access card (e.g., employee badge), or an NFC capable Android phone with a supported USB card reader. [Note: The system can support multiple badges for each user if desired].
3. The user may use the Xerox[®] Workplace App, using any of the following methods:
 - a. Supplying the 4-character code found on the local user interface of the machine into the Workplace App. This identifies the printer in the App and the user can confirm that they wish to unlock the device.
 - b. Tapping the NFC tag of the printer using their mobile phone (Android or iPhone 7 or newer with iOS 11).
 - c. Scanning a QR Code (found on the Welcome Page or on the blocking page for AltaLink devices).

In each of the above scenarios, upon supplying valid credentials or making the unlock request, the printer removes the blocking screen and the user has access to the services / features of the printer. If the printer is an EIP capable device and the Print Client App is installed, then the user may select the App and view their list of jobs without providing additional login credentials for the app.

In conjunction with authentication feature, the Xerox[®] Workplace Suite supports a feature called Auto-Release. This feature is disabled by default but may be enabled by the Administrator. Upon successfully completing the authentication step at a printer, if the Auto-Release feature is enabled, any print jobs uploaded to the system are automatically be released and printed at the device.

Xerox[®] Workplace Suite: Printer Client App

Devices which are EIP capable have the ability to support the Xerox[®] Workplace Suite App Authentication Solution. This App allows users to identify themselves, view and manage their print jobs.

The Workplace Suite Server installs the EIP App on the printer using the EIP Registration API, which is done using HTTP/HTTPS. Communication between the EIP App and the Workplace Suite Server is done using HTTPS over port 443. For older legacy devices that do not support HTTPS or are not able to handle the encryption keys used by the WS server, the option exists to enable the App to use HTTP over port 80 on a printer by printer basis.

Xerox Apeos

Fuji Xerox[®] multifunction devices introduce a flexible proprietary platform called Apeos. This platform acts as a secure embedded web service that other applications can leverage to expose functionality and services to the user through the local control panel interface. The Xerox[®] Workplace Suite uses this platform to secure access and present users with the Xerox[®] Workplace Suite solution for the Mobile Print Workflow. [The Print Management Workflow does not support Apeos].

Customer Email Server(s)

The email server is used to receive emails from and send emails to users of the Workplace Suite solution. The preferred implementation is to leverage the client's established email infrastructure and email security in place; however, the mail server can be an internally or externally managed server. The email infrastructure acts as the path to transport user's documents into the Xerox[®] Workplace Suite infrastructure. The user's documents temporarily reside on the mail server until the email message and its attachments are retrieved by the Xerox[®] Workplace Suite server.

The Xerox® Workplace Suite administrator will need to configure both the incoming mail server as well as the outgoing mail server. Both connections require credentials (e.g., username / password) to access the mail servers. The setup, maintenance, and security of the customer email server is outside the scope of Xerox® Workplace Suite.

Network Appliance

The network appliance, sometimes referred to as an ID Controller, is an external hardware device that supports the ability to plug in a USB keyboard mode card reader and transfer card information to a configured application. In this case, the Network Appliance is configured to send card data to the Workplace Suite Server.

The network appliance and the Agent communicate via raw TCP sockets with proprietary data exchange based on the manufacturer of the appliance.

Elatec: The Elatec TCP Conv and TCP Conv2 use ports 7778 and 7777 respectively. The card data is sent in plain text.

RF Ideas: The RF Ideas Ethernet 241 uses port 2001. By default, the card data is not encrypted, but the option to use encryption is available.

Xerox® Services Manager

The Xerox® Workplace Suite can connect to Xerox® Services Manager (SM) in order to perform the following actions:

- Export Job Data (Page count, Plex, etc.)
- Import Printers, Sites and Printer/Site Mappings

Each of these methods of synchronizing with SM has its own configuration as well as specific limitations on the system as a whole.

Connectivity to SM can only be enabled if Xerox® Workplace Suite has a license for “Xerox® Workplace Suite – Managed Print Services.”

Export Jobs to Xerox® Services Manager

Only the account ID is needed in order to export jobs to SM. If the printer data is matched to a printer in SM, then SM records the data.

If “Obscure User Data” is enabled, no identifying user information such as the username or password is sent to SM. All identifying information is replaced by unique GUIDs such that the number of individual users reported remains the same but each unique user cannot be identified.

The following data is sent to SM:

Display Name

- Printer Display Name

Network User Name (e.g., the Domain\Username)

- If Obscure User Data is set, a random GUID is sent
- If Obscure User Data is not set, the Domain\Username is sent

Email Address

- If Obscure User Data is set, a random GUID is sent
 - Network Accounting ID and User Name
 - NUp
- This only applies when printing using the FX Apeos workflow
 - Job ID
 - Job Type
 - Copies
 - Page Count B/W
 - Page Count Color
 - Total Page Count
 - Plex
 - Submission Date Time
 - Completed Date Time
 - Content Size
 - Color
- If the document contains color
 - Duplex
 - Document Name
 - Document Type
- If the document is Word, PPT, etc.
 - Media Size
 - Printer Name
 - Printer MAC Address
 - Server Name
- Always Workplace Suite Server Name
 - Server MAC Address
- Always Workplace Suite Server MAC address
 - PDL Type
 - Fax Destination Number
 - Fax Duration
 - Scan Recipient Description
 - Scan Recipient Type
 - Device Job Completion Time

Import Printers / Sites from Xerox® Services Manager

When the Xerox® Workflow Suite is configured to import printers and sites from SM, then SM is treated as the source of record. As such, the administrator has several limitations on what can be modified on printers and sites. The general principle is that any data that comes from SM will be

read-only. The administrator can only change fields related to printers and sites that do not come from SM.

When printers are imported from SM, Xerox® Workplace Suite performs an SNMP discovery to add the printers to the printer list. If the discovery fails, printers are not added to the system.

In order to correctly discover SM printers, discovery settings such as SNMP community names and device credentials must be set correctly on the discovery tab. The settings that the printers used to discover the printers from Xerox® Device Manager or Xerox® Device Agent are not used and must be specified again in Xerox® Workplace Suite.

If a printer is successfully imported in Xerox® Workplace Suite and is then deleted from SM, it remains in the Xerox® Workplace Suite until the system administrator disables or deletes it.

App in the Gallery

This item refers to an App in the Xerox App Gallery that has been modified to use the Single Sign-On feature provided by WS and is running on the EIP browser of the printer. The App is expected to retrieve configuration from the printer and pass this back to the App Server so that it can determine if the SSO feature is supported by the WS server. The App and EIP browser act as an intermediary between the App Server (usually outside the corporate firewall) and the WS server, which is typically on the internal customer network. All communication between the App, the App Server and the WS server uses TLS. [Note: the App is not written by or controlled by the WS solution. It is an external component to the system that is making use of functionality provided by the WS.]

App Server

The server hosting the functionality supplied by an App in the Gallery. This may be a Xerox hosted server or a third-party server, depending upon who created the App. The App Server never directly communicates with the WS. All communication is funneled through the instance of the App running on a printer and the EIP browser of that device. Communication between the App Server and the App uses TLS. [Note: The App is not written by or controlled by the WS solution. It is an external component to the system that is making use of functionality provided by the WS.]

User and Email Server Communication

The first layer of security is at the point of contact between the user and the method used to expose the email address to the end user. Although this is necessary to facilitate the use of the system, it can be controlled using various mechanisms. For example, the email address can be made available through a Xerox printer's EIP interface and thus accessible to only people physically at the printing device.

The details on how the XMPS solution interacts with the customer email server are provided later.

Users submit their documents for printing using standard email messages from their smartphone to their company's email server. Whether the email messages are encrypted or not is a decision and responsibility of the company's IT department.

If the user is submitting the email within the internal corporate network to a corporate email server, the transmission of the document is as secure as any email sent over the corporate network. This is true for both wired and wireless connections. However, if the user submits the email from outside the corporate network, for example, sending it from a personal email account such as Gmail, security cannot be guaranteed until the email is within the corporate network.

In both cases, the security of the document is no different than any email sent to a co-worker's corporate email address.

While a public email server can be used, it is recommended that you have control over the email server and that it is within your corporate firewall. This latter configuration offers the first line of defense by giving you the ability to create and control Blocked and Allowed user lists based on email domain.

The Workplace Suite Server communicates to the end user via email messages sent through the customer's email server. Each time a user submits documents for printing; the Workplace Suite Server retrieves the message and responds with a confirmation email message. The confirmation email message contains a personal confirmation code. The confirmation code is later used to retrieve and print their documents at the multifunction device (MFD).

Confirmation codes are configurable in length and unique for each user. Once assigned the confirmation code will be reused for each submission from the same user. Note, this is specifically for the user's convenience so that all their jobs will be shown at the MFD. Users may request that their confirmation code be changed at any time.

Xerox® Workplace App and Xerox® Workplace Suite Service

In order for a smart device application, running on a service provider's 3G/4G/LTE network to "talk" to a server behind a corporate firewall, an intermediate cloud-based service is used. Xerox uses the Microsoft Azure Service Bus Relay to create this cloud endpoint between the mobile device and the Workplace Suite Service.

The HTTPS protocol is used for all communications between the Workplace App, the Xerox managed cloud-based routing service, and the Workplace Suite Service. Validation of the certificate is done by the receiving system. Therefore, the Xerox managed cloud-based routing service relies on the mobile device operating system to validate the security certificate as part of establishing the TLS connection. Likewise, the Xerox managed cloud-based routing service relies on the Workplace Suite Service to validate the security certificate as part of establishing a TLS connection.

The Workplace App requires users to authenticate before using any of its features. Basic authentication is performed with the Mobile Workplace App providing email and confirmation number or using LDAP credentials over the HTTPS (TLS) protocol.

If using the Chromebook or Chrome browser Workplace Mobile (Print Portal) extension with the single sign-on feature, when a user attempts to log in, the app pre-populates the email field with the logged-on user's email address. When this is submitted to the server, the app also includes the Google authentication token of the logged-on user as well as the AppID of the Workplace App. The server validates the email, token and AppID with Google using HTTPS over port 443. If these are valid, the user is considered authenticated. The server then creates a Mobile Print authentication token and returns that to the Workplace App. The user then remains logged into the App until the Mobile Print token expires. At this time, the app attempts to repeat the process.

Once authentication is complete, data is passed directly between the Workplace App and the Workplace Suite Server or from outside the corporate network by routing through the Azure Service Bus Relay. This includes all data for previewing and printing jobs, location of printers, and user location data as determined by the mobile device. Users are only able to access documents they submitted. Again, all communication is using the HTTPS protocol.

In a DMZ Configuration, the intermediate cloud-based service is hosted by the customer. The Workplace App communicates with the customer hosted cloud service, which in turn communicates with the Workplace Suite Server. All communication between the mobile phone and the DMZ

server, as well as the DMZ server and the Workplace Suite Server is done using HTTPS. All other details in the above section apply to a DMZ setup except for the replacement of the Xerox hosted cloud service with the customer hosted DMZ server.

If using iOS native printing, the Workplace App may use mDNS (Port 5353) to discover printers (e.g., the Xerox® Workplace Suite server). When iOS Native Printing is enabled, the Workplace Suite Server is listening for and responding to mDNS queries. Alternatively, the Workplace App may use DNS-SD (Service Discovery) to locate printers. Once found, the Workplace App uses the iOS native print submission mechanism (IPP over port 631) to upload jobs to the Workplace Suite Server.

Customer Email Server and Xerox® Workplace Suite Service Communication

Network communication between the email server and the Mobile Suite Server is configured within the administration pages.

For security:

- The Workplace Suite server requires a customer supplied username and password to access the Mail Server. The credentials are stored within the SQL database.
- The communication port is configurable.
- Network communication between the servers can be configured to be encrypted using TLS.

The Workplace Suite server can send emails to the user and acts as a standard email client. It periodically polls the email server (the poll time is configurable) and retrieves any emails and attachments as needed. Once the email is retrieved, the email and attachments on the email server are deleted.

The Xerox® Workplace Suite server supports connectivity to the following:

- SMTP (port 25 or 587),
- IMAP (143 or 993 (TLS)) and
- POP (110 or 995 (TLS))
- Microsoft Exchange Web Services (80 or 443 (TLS))
- Lotus Domino NRPC (Port 1352)

Using the protocols above, the Workplace Suite connects to the inbound email account to pull messages and use the outbound email configuration for sending email. The inbound and outbound email configurations may use different protocols. Workplace Suite can connect to a Microsoft Exchange Server 2007 or later using Exchange Web Services (EWS). This connection is made over the HTTPS protocol. When communicating with Domino, the WSS communicates using a local API with Lotus Notes Client installed on the same PC as WSS, which in turn uses Note RPC to communicate with the Domino server.

The Workplace Suite Server can authenticate either using Basic Authentication or Impersonation.

In the case of basic authentication, the username and password are sent securely to the EWS server for authentication.

When impersonation is used, the Workplace Suite will Log On as the impersonated user for the duration of the EWS connection. The impersonated user must have Log On credentials to the Workplace Suite system.

Workplace Suite Server and Printer Communication

The Workplace Suite server communicates with the Printer for a number of different reasons using various protocols. These are outlined below:

Discovery

Discovery applies to all printers that are enabled to work with Xerox® Workplace Suite. The Workplace Suite Server connects to the printer via SNMP (Port 161) to retrieve printer configuration, capabilities, paper tray information (paper size and availability). The SNMP communication is done either via SNMPv1/v2 (no encryption) or SNMPv3 (encryption) using port 161.

Printer Client (EIP App)

The Workplace Suite connects to the printer's web services to install the Printer Client EIP/Apeos application on Xerox printers via port 80 (HTTP) or 443 (HTTPS) based on the configuration of the printer. The Server makes use of the EIP Session API and Device Configuration APIs using these same ports.

The Workplace Suite can host web pages to the printing device's User Interface commonly referred to as Xerox Extensible Interface Platform® (EIP) and Apeos. The device must be enabled to display these web pages and the web pages do not have any access to documents or any data residing on the printing device. All data exchanged is over port 80 via HTTP (default). HTTPS (port 443) unless the printer is specifically configured to use HTTP (port 80).

Based on the configuration of the system, users may need to identify themselves using the Printer Client. This done by entering their confirmation number, primary PIN, email and confirmation number, or their LDAP credentials based on the system configuration. The LDAP password is always obscured (hidden) when entered in the application. The confirmation number is shown by default, but the option to obscure the confirmation number may be enabled by the administrator if necessary. The primary PIN is always displayed.

Print Authentication

Authentication is only supported by Xerox® multifunction devices that support the EIP Convenience Authentication API.

The server configures the authentication feature on the printer via SNMP (Port 161). The SNMP communication is done via SNMPv1/v2 (no encryption) or SNMPv3 (encryption).

During user authentication, the Workplace Suite Server and the printer communicate using web service calls to initiate an authentication session, supply card data, and / or prompt the user to supply credentials or other data, and unlock the device for user access. All data exchanged is over port 443 via HTTPS.

Scan and Copy

For Scan and Copy jobs processed by WS, the scan job is transferred from the printer to the server using HTTPS (or HTTP if HTTPS is not available). The server initiates this transaction, so the job is pulled to the server. In the case of Copy jobs, the WS server sends the job back to the printer using the configured print protocol for that device (LPR / RawIP / IPP over SSL).

Administrator Configuration and the Workplace Suite Server

In order to administer the Workplace Suite server, users connect to the server using a web browser. When the system is first installed and not yet configured, the system will be in an open state, allowing any user to connect and configure the basic system using the Install Wizard. This process also requires the configuration of an initial starting administrator by supplying their email address and assigning them a confirmation number. Once the Install Wizard is complete, users log into the system using the configured authentication mechanism for the User Portal. The supported methods for authentication include:

- Email and Confirmation Number
- LDAP/AD User Credentials
- Windows Integrated Authentication

For Windows Integrated Authentication, Workplace Suite will use the identity of the current Microsoft Windows session to look up the user in the SQL database. If the user exists, then they are logged into the User Portal without having to provide credentials. If the user does not exist, then they will be blocked from accessing the web interface. [Note: If IIS web server on the XWS system is unable to validate the identity of the logged-on user, then they may be prompted to supply Windows credentials.]

The administrator may assign roles to the users of the system, such as “General User” or “System Administrator”.

Document Conversion Server and Workplace Suite Service Communication

The Workplace Suite service sends the user’s Mobile Print Workflow documents to the Document Conversion Server using a named pipe (net.pipe) protocol on port 8802. The connection can be configured to use other bindings if desired. User documents are only temporarily stored within the external Conversion Server and only to the extent of network communication and conversion.

When the Workplace Suite Service and the Conversion Server(s) are on separate machines, they communicate via TCP/IP over ports 8801 and 8802.

Document Conversion Server and the Printer

The Conversion Server which hosts the Document Conversion Engine (whether running on the same server as the Workplace Suite Service or on a separate server) is responsible for submitting the converted Mobile Print job to the printer. The default submission method for Mobile Jobs is Raw IP (Port 9100) over TCP/IP. Other ports that can be used are 2501, 2000, 515 (LPR), and 443 (IPP over TLS).

User Workstation and Print Server Communication

The user workstation communicates with the print server in two ways:

- Print queue and driver install
- Print submission

Print queue install can be initiated via the Workplace Client, or via the Windows print install wizard if print queues are added manually. Printing is done via traditional shared Windows network printers. These capabilities use DCE/RPC communication over port 1058 and SMB communication via port 445.

Job Agent Service/Client and Xerox® Workplace Suite Server Communication

The Job Agent runs either on the user's workstation (Job Agent Client as part of the Workplace Client) or on a Print Server (Job Agent Service).

Job Agent Service Start Up

When the Job Agent Service is first installed, the software listens on port 443 using HTTPS for initial configuration information from the Workplace Suite Server. Once the administrator adds the IP address of the external print server to its list of supported servers, the Workplace Suite Server pushes the communication endpoint to the Job Agent Service. This endpoint is used for all communication between the Job Agent Service and the Workplace Suite Server. The JAS processes incoming jobs if Content Security is enabled, looking for matches to any of the Content Profiles. If a matching profile has content storage enabled, the JAS creates a PDF copy of the job. The results of content matching and any PDF copies are transferred to the WS server.

Job Agent Client Configuration

The Workplace Client periodically polls the Workplace Suite Server using the configure endpoint with HTTPS on port 443. This includes the retrieval of timers for job polling, configuration polling, Content Profiles, and maintenance polling. Optionally, the Workplace Client can also be configured to listen for message notification being sent from the Workplace Suite Server. This lessens the amount of network traffic generated using the Workplace Client. When running in the messaging mode, the Job Agent Client (JAC) listens on port 9807 using UDP by default. If this port is not available, the client tries 3 other ports to find one that is not in use, adding 10 each time (e.g., 9807, 9817, 9827 and 9837). If the client fails to obtain a port, then it defaults to using polling when querying for pending jobs. The JAC processes incoming jobs if Content Security is enabled, looking for matches to any of the Content Profiles. If a matching profile has content storage enabled, the JAC creates a PDF copy of the job. The results of content matching and any PDF copies are transferred to the WS server.

Job Management

Both the Workplace Client and the Job Agent Service communicate with the Workplace Suite Server to communicate new jobs being added to the system, to know when jobs are to be released, to update job status, and job synchronization. This is done via web service calls using HTTPS over port 443. The Job Agent Service listens for notifications from the server about jobs to be released. The Workplace Client either polls for this information or if messaging is enabled it listens on port

443. The reporting of new jobs and job status is always initiated by the Workplace Client. For the Job Agent Service, communication is two-way.

Primary Print Server and Secondary Print Server

In the event that a customer has configured the use of 1 or more Secondary Print Servers to be used in conjunction with a Primary Print Server, the servers communicate together using port 443 and HTTPS for the purpose of facilitating workload distribution.

Job Agent Service and Printer Communication

When a job is released for printing, the Job Agent Service / Client submits a print ready file to the printer. The default submission method is Port 515 (LPR). Raw IP (Port 9100) over TCP/IP can also be used as well as IPP over SSL (Port 443). For Raw IP printing, the port is configurable.

External Communication Between Xerox® Workplace Suite Service and Xerox® Cloud Services

Except for incoming email, by default Xerox® Workplace Suite cannot be accessed from outside the company network. The administrator enables this workflow and may choose to limit it to only users which are operating within the company network.

The Windows Azure Service Bus is a Microsoft Cloud based messaging system that Xerox leverages to establish a secure application to application connection allowing select communication between approved clients outside a company's network to leverage services within a company's solution. While the Windows Azure and Xerox hosted service provide the secure connection path to the service, access to the Xerox® Workplace Suite continues to be controlled by the local Workplace Suite solution. The Microsoft Azure Service Bus communication requires that the Workplace Suite server supports TLS 1.0.

Xerox® Services Manager and the Windows Azure Service Bus

During the provisioning process at set-up time an external URL is provisioned on the service bus then Xerox® Workplace Suite is configured to facilitate communication through that URL using an encrypted key. XMS initiates and maintains a connection to Azure service bus over HTTPS to XMS services so that users using their mobile device over a public cellular or Internet connection can use the Mobile Print Workflow. The URL endpoint assigned is what various end clients (i.e., mobile devices) connect to.

Mobile Devices and the Windows Azure Service Bus

When the mobile device communicates with XMS through the Azure service bus, communication is always over HTTPS with a secure trusted certificate over the service bus URL allocated in the provisioning process. To mitigate the need for the user to type in the URL, a routing mechanism was created to allow URL discovery based on the user's email address domain. Users may be prompted for a company code if the login service is unable to determine which company they are associated with using the domain. Company code is used as a deciding factor to which account/service the user will authenticate/route against. Users have an option to always prompt for company code inside the settings view during login. This gives greater flexibility for a user to specify a certain company to be routed to upon login. The discovery and routing are facilitated through a Xerox® managed cloud-based routing service, which is discussed in the next section.

Mobile Devices and the Managed Cloud Based Routing Service

Mobile devices or other user interfaces may connect to the Managed Cloud Based Routing Service to determine what cloud endpoint is used for the remainder of the mobile print session. The routing service determines the cloud endpoint by the user's email address. If this service cannot resolve the external endpoint it may prompt the user for their company code to further resolve the cloud external endpoint. All communication between the mobile devices and managed cloud-based routing service is secure over HTTPS (port 443) with a trusted certificate.

Xerox® Workplace Suite and LDAP / Active Directory Communication

LDAP / Active Directory Authentication

When configured for Enterprise Authentication, Workplace Suite verifies user credentials against Active Directory. Workplace Suite also queries Active Directory for information regarding trusted domains.

In order to communicate with Active Directory, Workplace Suite uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Workplace Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389, or via 636 if TLS is being used. Communication is secured via SASL bind using the GSSAPI mechanism.

Active Directory Import

Xerox® Workplace Suite can be configured to import users from Active Directory. This capability is an extension of the setup used for LDAP / ADS Authentication. The Admin has the ability to configure the type of LDAP access (Anonymous, Basic, Negotiate) required when connecting the LDAP server. By default, the system is configured to use the Negotiate setting, which in turn instructs the Workplace Suite Server to use SASL when doing an LDAP Bind.

The Admin must supply user credentials that are in turn supplied to the LDAP server when performing an import (assuming they have selected either Simple or Negotiate for the Usage Mode). The credentials are stored in the Workplace Suite Server database (SQL), and are encrypted using SHA256 and AES.

As part of the import, the Admin can define the LDAP containers that are to be queried as part of the import and, in turn, map the fields within those containers to fields within the Workplace Suite User Database.

In order to communicate with Active Directory, Workplace Suite uses the Active Directory Services Interfaces (ADSI) technology that is available in all Windows Operating Systems supported by Workplace Suite. The communication with the Active Directory servers occurs via the standard LDAP port 389 or via 636, if TLS is being used.

Active Directory On-Boarding Using Email

When a new user sends an email, Workplace Suite checks all of the domains configured for "Advanced" or "Advanced with Import" for the user entry matching the user's email address. If the user is found in Active Directory, Workplace Suite populates the user database with the data found in Active Directory.

Communication Between Xerox® Workplace Suite and Xerox® Service Manager

The Workplace Suite system can be configured to connect to SM in order to perform the following actions:

- Export Job Data (Page count, Plex, etc.)
- Import Printers, Sites and Printer/Site Mappings

Each of these methods of synchronizing with SM has its own configuration as well as specific limitations on the system as a whole. Connectivity to SM can only be enabled if Workplace Suite has a license for “Managed Print Services”. The Importing of Printers and Sites requires the SA to configure an Account ID as well as a Username and Password. Optionally, a Chargeback Code may be specified. For the Exporting of Job Data, the Admin need only configure the Account ID. They may optionally enable the “Obscure User Data” setting, which when enabled obfuscate all user data (e.g., User Name, Email Address, Accounting User Name before sending any data to the SM server.

All communication between SM and Xerox® Workplace Suite is over HTTPS (port 443).

Communication Between Xerox® Workplace Suite and Workplace Suite Reporting Service in Azure

The Workplace Suite Server collects system usage information on a daily basis and report this to the Workplace Suite Reporting Service, an online Xerox service. The type of information being collected includes, but is not limited to, items such as:

- Version of Workplace Suite Software
- Type of SQL Database
- Associated Licenses
- Printer Details:
 - Number of Printers
 - Features that are enabled (Mobile Print, Authentication, Desktop Print, Printer Client, etc)
 - Xerox vs Non-Xerox
- Server Details
 - Operating System
 - Size of Memory
 - 32 vs 64 Bit
 - Microsoft Office: Installed, Activation State, Version
- Print Queues:
 - Number and Type (Outgoing, Incoming, Client, Network, Conversion Mode)
- Prints:
 - Number Succeeded, Failed, Deleted or Expired.
 - Release Mechanism: Email, Printer Client, Mobile App, Auto Release.
 - Print Job Summary: Number of Color Pages, Number Black & White Pages.
 - Document Types: Word, Excel, Power Point, etc.

Information is used to improve Xerox customer support as well as the performance and functionality of the product in future releases. No personal or customer sensitive information is collected.

This feature is enabled by default but may be disabled by the customer if desired. This setting resides on the following page: Company > Maintenance > System Health Dashboard > System Utilization.

Communication Between the App from the Gallery, the App Server, and the Xerox® Workplace Suite Server

All SSO related communication requests to get or set a user's authentication data uses TLS. Sensitive information in all communications is also encrypted at the message / data item level in addition to the encryption of the data stream itself using TLS. Message level encryption uses shared keys pairs (a public and private key) for exchange of data between the WS Server and the App Server. Data is both encrypted and signed to ensure authenticity and privacy. Encryption is done using an RSA algorithm with key size of 10240. Additional details on SSO can be found in section 7.9 Single Sign-On of this document.

5. Logical Access, Network Protocol Information

Protocols and Ports

The following table lists the standard default ports used by the Xerox® Workplace Suite. Some port numbers are configurable on the printer, such as the Raw IP printing port. Other port numbers are non-configurable and cannot be changed.

Xerox® Workplace App Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTPS using TLS	TCP 443	Authentication, Job / Printer Listing, Initiate Print Conversion	Non-configurable	App to WS Service	Out

Xerox® Workplace Suite Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
Azure Service Bus	TCP 80, 443	Handling Mobile App requests: Authentication, Submission, Job Listing, Print Release	Non-configurable	WS to ASB	Out
Cloud Routing Service	TCP 443	Store or update mobile routing information for phone communication	Non-configurable	WS to Cloud Routing Service	Out
DCE	TCP 8801, 8802	WS and DCE Communication	Configurable	WS to DCE	Out
HTTPS	TCP 443	WS uses this port to communicate with other WS servers. JAS and JAC also request info using this port.	Configurable	WS / JAS / JAC to WS	Out
HTTP	TCP 80	WS uses this port to notify JAC	Non-configurable	WS to JAC	Out

Protocol	Transport and Port Value	Use	Option	Component	Direction
		that a job is ready to be released			
SQL	TCP 1433	Microsoft SQL Client to Server Communication for database queries and storing.	Non-configurable	WS to SQL Server	Out
LDAP	TCP 389	Authentication, User Look-up	Non-configurable	WS to ADS Server	Out
LDAPS	TCP 636	Authentication, User Look-up.	Configurable	WS to LDAP Server	Out
HTTPS using TLS	TCP 443	EIP Registration, Configuration, Accounting, Scan Job Retrieval (Note: HTTPS preferred)	Non-configurable	WS to Printer	Out
HTTPS	TCP 443	Print Authentication (Convenience Authentication)	Non-configurable	WS to/from Printer	In/Out
HTTP	TCP 80	EIP Registration, Configuration, Accounting, Scan Job Retrieval (Note: HTTPS is used if enabled on the printer)	Non-configurable	WS to Printer	Out
SNMP	UDP 161	Printer Discovery, Configuration	Non-configurable	WS to Printer	Out
HTTPS using TLS	TCP 443	Send Print History and Retrieve Printer List to/from Xerox® Services Manager	Non-configurable	WS to SM	Out

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTPS using TLS	TCP 443	Send system utilization information to the Workplace Suite Reporting Service (MSRS)	Non-configurable	WS to MSRS	Out
SMTP	TCP 25	Sending email responses	Non-configurable	WS to SMTP Server	Out
SMTP / TLS (Secure SMTP)	TCP 465	SMTP over TLS. TCP port 465 is reserved by common industry practice for secure SMTP communication using the TLS protocol.	Configurable	WS to SMTP Server	Out
POP3	TCP 110	Post Office Protocol version 3, enables “standards-based” clients such as Outlook to access the email server.	Configurable	WS to POP3 Server	Out
POP3 / TLS	TCP 995	POP3 over TLS uses TCP port 995 to receive encrypted email messages.	Configurable	WS to POP3 Server	Out
Exchange Web Services	TCP 443	Exchange Web Services used for receiving Email	Configurable	WS to Exchange	Out
IMAP	TCP 143	Internet Message Access Protocol version 4, may be used by	Configurable	WS to IMAP Server	Out

Protocol	Transport and Port Value	Use	Option	Component	Direction
		“standards-based” clients such as Microsoft Outlook Express to access the email server.			
IMAP/TLS	TCP 993	IMAP4 over TLS for securely receiving encrypted email messages.	Configurable	WS to IMAP Server	Out
NRPC	TCP 1352	Lotus Notes RPC. This is the API used between Lotus Notes and the Lotus Domino server. Communication between WS and Lotus Notes is via a local API on the same PC.	Non-configurable	WS (running Lotus Notes) to Domino Server	Out
HTTP / HTTPS	TCP 80 / TCP 443	Administration using Web Admin Tool. If a certificate is already configured on the IIS default website it is used by Xerox® Workplace Suite. If no certificate is configured, WS creates a self-signed cert. The administrator has the option to load a certificate from a trusted	Non-configurable	Browser to Workplace Suite Service	In

Protocol	Transport and Port Value	Use	Option	Component	Direction
		authority later if desired.			
HTTPS	TCP 8443	HTTP over TLS. Used to activate or validate a license. If the customer is using off-line activation, then this port is not needed.	Non-configurable	Workplace Suite Service to Xerox® Licensing Server	Out
IPP	TCP 631	Receipt of Mobile Jobs on phones using the iOS Native Print feature. Always uses TLS.	Non-configurable	Mobile Phone to WS	In
HTTPS	TCP 443	HTTP over TLS. Used to validate a Chrome browser or Chromebook single sign-on user with Google.	Non-configurable	WS to Google	Out
App Socket RAW or Windows TCP-Mon	TCP 9100	Print Submission of Copy Jobs	Configurable	WS to Printer	Out
LPR	TCP 515	Print Submission of Copy Jobs	Non-configurable	WS to Printer	Out
IPP over TLS	TCP 443	Print Submission of Copy Jobs. Encrypted print transfer.	Non-configurable	WS to Printer	Out
HTTPS	TCP 443	Single Sign-On requests.	Non-configurable	WS <-> Printer	In/Out
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to WS	In

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2	Configurable	Network Appliance to WS	In
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to WS	In

Document Conversion Engine Server Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
App Socket RAW or Windows TCP-Mon	TCP 9100	Print Submission	Configurable	DCE to Printer	Out
LPR	TCP 515	Print Submission	Non-configurable	DCE to Printer	Out
IPP over TLS	TCP 443	Print Submission. Encrypted print transfer	Non-configurable	DCE to Printer	Out
DCE	TCP 8801, 8802	WS and DCE Communication	Configurable	WS to DCE	In

Print Server Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
SMB Print	TCP 445	Print submission to a network queue. Client Workstation to print server.	Non-configurable	Workstation to Print Server	In
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download. From Workstation Print Queue to Print Server or from Workplace Client to Print Server.	Non-configurable	Workstation to Print Server	In

Printer and Printer Client (EIP App) Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
HTTP / HTTPS	TCP 80 / 443	Retrieval of EIP Browser pages for display on the UI. Uses HTTPS by default. Authentication, Job Listing, Initiate Print Conversion	Non-configurable	Printer EIP App to WS Service	Out
HTTPS	TCP 443	Printer Authentication	Non-configurable	Printer to/from WS	In/Out

Job Agent Service Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw IP	TCP 9100	Print Submission	Configurable	JAS to Printer	Out
LPR	TCP 515	Print Submission	Non-configurable	JAS to Printer	Out
IPP over TLS	TCP 443	Print Submission	Non-configurable	JAS to Printer	Out
HTTPS	TCP 443	Configuration, Job Information, Print Release	Configurable	WS to/from JAS	In/Out

Job Agent Client Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw IP	TCP 9100	Print Submission	Configurable	JAC to Printer	Out
LPR	TCP 515	Print Submission	Non-configurable	JAC to Printer	Out
IPP over TLS	TCP 443	Print Submission	Non-configurable	JAC to Printer	Out
DCE/RPC	TCP 1058	Network Print Queue Access and Driver Download.	Non-configurable	Workplace Client to Print Server	In

Protocol	Transport and Port Value	Use	Option	Component	Direction
		From Workplace Client to Print Server.			
HTTPS	TCP 443	Configuration, Job Information, Print Release	Configurable	JAC to WS	Out
Raw	UDP 9807	Notification of Print Job Release	Configurable	WS to JAC	In

Network Appliance Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
Raw	TCP 7778	Receive Card Swipe Data from Elatec TCPConv	Configurable	Network Appliance to WS	Out
Raw	TCP 7777	Receive Card Swipe Data from Elatec TCPConv2	Configurable	Network Appliance to WS	Out
Raw	TCP 2001	Receive Card Swipe Data from RFIdeas Ethernet 241	Configurable	Network Appliance to WS	Out

iOS Native Printing Ports

Protocol	Transport and Port Value	Use	Option	Component	Direction
DNS-SD	UDP 53	Mobile Phone printer discovery using DNS.	Not-configurable	Phone to DNS Server	Out
mDNS	UDP 5353	Mobile Phone printer discovery on the local subnet using mDNS.	Not-configurable	Phone Broadcast on Local Subnet	Out
IPP	TCP 631	IPP Print submission	Not-configurable	Phone to WS	Out

Protocol	Transport and Port Value	Use	Option	Component	Direction
		to Xerox® Workplace Suite. Always uses TLS.			

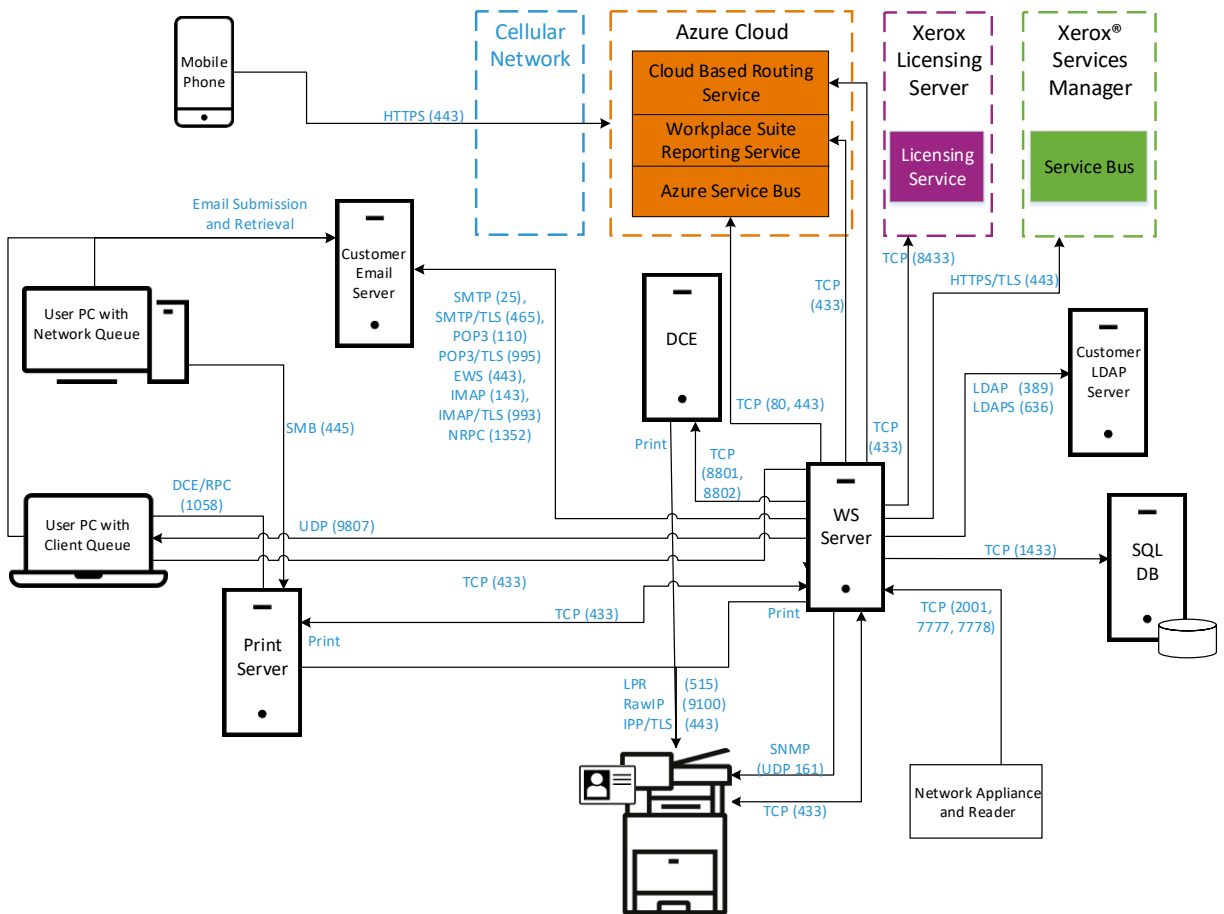
The default port for hosting application web pages is 443 using HTTPS. If HTTPS cannot be used (for example, it is prohibited in a specific region), HTTP over port 80 can also be configured. Both ports can run simultaneously.

Port Diagram

The following diagram gives a pictorial representation of the components and ports being used to facilitate communication.

Network Port Diagram

Xerox® Workplace Suite – Network Port Diagram



6. System Access

Xerox® Workplace Suite (Web Administration Portal)

When accessing the Xerox® Workplace Suite directly (i.e., the User Portal for administrative access), the administrator connects to:

`https://<webserver address>/Login/`

The user provides credentials to log into the User Portal based on the configured authentication type:

- Email and Confirmation Number
- LDAP Authentication
- Windows Integrated Authentication

The user must exist in the WS user database and must be assigned the “administrator” role.

For Windows Integrated Authentication, Workplace Suite will use the identity of the current Microsoft Windows session to look up the user in its SQL database. If the user exists, then they are logged into the User Portal without having to provide credentials.

Xerox® Workplace App (Print Portal)

When accessing the Workplace App, users need to provide their email address. WS looks up the user’s email address to determine the company account to which they are homed, and then based on that company’s authentication configuration, they are prompted to enter either their Xerox® Workplace Suite Confirmation Number, or their company LDAP credentials (DOMAIN\USERNAME and PASSWORD). When using LDAP, the Domain is used to route the LDAP requests to the correct Agent, which in turn communicates with the ADS/LDAP server.

The results of successfully authenticating with WS is an access token. The token is stored on the phone and used for subsequent communication with WS. The lifetime of the access token is configurable. Prior to the token expiring, the phone obtains a new token, which requires the use of the user’s login credentials. The Workplace App stores the user’s access credentials on the phone in encrypted format in order to support renewing the access token. For Android devices, the credentials are encrypted and saved to internal storage of mobile device and this is only accessible by the Workplace App. For iOS devices, the credentials are saved in a keychain which is encrypted and only accessible by the Workplace App. The OS of the mobile device deletes any saved data including the credentials when the application gets un-installed.

Some customers have security concerns about providing authentication credentials (even though they are always encrypted) on their mobile phone using the internet or through their wireless provider (3G/4G). For accounts with this concern, the WS provides a configuration option which forces Workplace App user authentication to take place only on the corporate LAN. Once authentication has taken place, users are then allowed to use the app on networks outside of their company LAN for printing. This option is disabled by default.

Workplace Client

The Workplace Client needs to access the enabled client-based queues hosted on the Print Server(s) in order to download and install the print driver for each client queue. By default, the Workplace Client runs as an NT Service on the workstation and uses the Local System Account when attempting to connect to the Print Server hosting the client queue. If these credentials are not valid, the user may supply different credentials using the Sys Tray utility installed with the Workplace Client. The supplied credentials are then used by the Workplace Client NT Service when accessing the Print Server queues to retrieve the driver. Credentials are stored in the system registry of the workstation. The password is encrypted using SHA1-AES.

Print jobs submitted via the Workplace Client always use the network username of the person logged into the workstation as the job owner.

Printer Client (EIP App)

To access the Printer Client App, users either need to log into the printer via the Convenience Authentication feature and then select the Printer Client App, or they need to log into the EIP App itself. The Workplace Suite administrator also has the option of allowing an external authentication mechanism (something other than the Workplace Suite itself) as an approved authentication service. So a user can authenticate themselves at the printer with the external service, and if they then select the Workplace Suite Printer Client App, the App pulls the logged on users credentials from the session (network username and email address) and if these values map to a user in the Workplace Suite database, then the user has access to their print job(s) for release at the device. [Note: the ability to use an external authentication mechanism is off by default].

The Printer Client (EIP App) never saves the user's credentials. The user can log out of the EIP App manually but selecting the "Exit" button in the App, or by navigating out of the App (e.g., selecting the All Services, Machine Status, or Job Status buttons on the UI panel). The UI itself has a built-in inactivity timer that logs the user out if the user is not interacting with the UI. The inactivity period is configurable by the device administrator. In addition to the device timer, the EIP App itself has its own 5-minute timer. The EIP App timeout logs the user out of the App after 5 minutes of use, unless they dismiss warning pop-up, which restarts the 5-minute timer.

User Portal

When accessing the User Portal, users connect to:

<https://<webserver address>/Login>

The user must exist in the WS user database, and the user record must be enabled and not locked out. The administrator can configure the type of authentication that will be required to access the User Portal. The supported methods include:

- Email and Confirmation Number
- LDAP Authentication
- Windows Integrated Authentication

For Windows Integrated Authentication, Workplace Suite will use the identity of the current Microsoft Windows session to look up the user in its SQL database. If the user exists, then they are logged into the User Portal without having to provide credentials.

The only setting or configuration available to the user using the User Portal is the configuration of Release Permissions for the Printer Client.

7. Additional Security Items

Auto Release via Network Appliance Workflow

Held print jobs are released automatically as soon as the user scans a card at a mapped network appliance associated with the printer.

Network appliances are small network boxes that attach to the network and permit Xerox® Workplace Suite to control the release of user documents to printers that do not support the use of Secure Access / Convenience Authentication. A network appliance is configured on the network by the administrator, the appliance is associated with the particular printer in the WS Admin Web Portal, and the user can release their jobs at the printer by swiping their card using the card reader associated with the printer. One network appliance is required for each printer.

Models

Three network appliance models are supported by WS:

- RF Ideas Ethernet 241
- Elatec TCP Conv2
- Elatec TCP Conv

Each of these models is available by default on the Workplace Suite Admin webpage at Account > Settings > Network Appliances > Models. If any or all of these models are not going to be part of your site installation, they can be disabled to turn the listeners off on the server.

The listeners use these default ports:

- RF Ideas Ethernet 241 - 2001
- Elatec TCP Conv2 - 7777
- Elatec TCP Conv - 7778

The default ports can be changed by the administrator if the network appliances on your system have been configured to use a different port. Any firewall on the Agent must be configured to allow communication through the port(s).

By default, the network appliances support communication using non-encrypted channels. Therefore, card data is sent in plain text format when transmitting the card data from the network appliance to the Agent. The RF Ideas Ethernet 241 is the only network appliance that supports encryption (using SSL) of the communication path.

Note: The Ethernet 241 supports SSLv3. It does not support TLS1.x.

Audit Log

The Xerox® Workplace Suite maintains a history of the users that have logged in WS via any of the interfaces: Workplace App, Printer Client, or Convenience Authentication. Entries are maintained for a period of 1 year. Entries older than that are purged from the log.

DMZ Configuration

The Azure service bus public endpoint is the typical configuration when a customer wants to allow users outside the network to access the Xerox® Workplace Suite. However, there are some customers who wish to allow users outside the company network to access the Workplace Suite, yet they do not want to allow documents to be passed through the Microsoft owned cloud.

Xerox® Workplace Suite supports a configuration where the customer can set up a satellite pass-through server in a DMZ, which is accessible from outside the network. This server is configured as the external endpoint in a private configuration, and all data sent to it is forwarded to the internal server.

The communication between DMZ servers and internal servers is secured. Before a DMZ server can communicate with an internal server, the DMZ server must authenticate with a valid username/password for the internal server. Once this authentication is successful the DMZ server receives a token that is used for all further communication. This token is required for all communication to the internal server.

DMZ Setup

In order to enable the DMZ feature, the Workplace Suite Server must be set to “Private” mode. When inside of your company firewall, Mobile App users are able to access WS via the Internal Server endpoint. When outside of the firewall, Mobile App users can access WS via the External Server endpoint.

DMZ Setup requires that a server be set up which has an external network connection to the Internet. The XMS software needs to be installed on this server and configured to support the DMZ feature. The setup entails pointing the DMZ server at your WS server and supplying administrator credentials which are used by the DMZ server when connecting to the WS server.

All DMZ configuration is done using HTTPS communication over port 443. The connection is initiated by the DMZ server, and can be trusted by the WS server based on the supplied administration credentials.

Mobile Devices and the DMZ Server

Mobile devices or other user interfaces may connect to the DMZ Server to access their Workplace Suite Server when they are external to the company's network.

All communication between the Mobile Print App and the DMZ Server is over HTTPS (port 443).

Mobile Login using a Company Code

The mobile app can be configured to prompt for a company code at logon time. When configured to do this, the app queries the Azure Service Bus to find the DMZ Server end point. After which, all communication between the mobile app and the Workplace Suite Server is directly between the mobile phone and the DMZ server. User validation of credentials and transmission of all jobs occurs between the phone and the DMZ Server.

Mobile Login using the Private Access Control

The mobile app can be configured with using the Private Access Control feature, such that the app points to the DMZ server for all communication. With this configuration, the mobile app never accesses the Azure Service Bus. To perform this setup in the mobile app, Users can manually enter the link (as provided by their Workplace Suite Administrator), or the Admin has the ability to push out an email to all users which includes a link that, when selected from a Mobile device, updates the configuration of the App and makes it point to the desired external URL.

Debug Logs

The Workplace Suite server uses logging to help diagnose issues and problems. User credentials (e.g., passwords or confirmation numbers) are never logged.

Workplace Suite Server Windows File Structure

The Workplace Suite Server stores files in the install location: %ProgramData%\Xerox\XMP

Smartcard (CAC/PIV) Integration

The Workplace Suite solution may be used with external authentication mechanisms, including CAC/PIV card authentication. Many Xerox advanced office products support smartcard integration, which is built into the Xerox® multifunction device (MFD) itself. Smartcard authentication is not performed directly within Xerox® Workplace Suite. Instead, the authentication of the user is performed between the printer, the smartcard and the Domain Controller at the customer site. The Xerox® Workplace Suite can be configured to allow users authenticated by an external system (i.e. something external to Workplace Suite) to access the printer client (EIP App) using the logged-on user identity. This removes the need for the user log into the Workplace Suite Printer Client. Users see their list of jobs after starting the app and may select and release them as desired.

The Workplace Suite server must be configured to allow the logged-on user (using an external authentication mechanism) to access the Printer Client. This is done using the following settings from the Web Admin Tool:

Company > Policies > Security > Printer Client

- Enable “Logged on Users (Access Card)”
- Enable “External Printer Authentication”.

The Workplace Suite server must also be configured such that the “Alternate Access Card User” field for each user in the User database is populated. Typically, this field is populated from LDAP using the UPN (universalprinciplename) field. In a typical customer environment using this capability, a user logged onto the Printer would normally have an identifier something like:

- username@domain (UPN)

When that same user submits jobs from their PC, the user identity is typically has a format of:

- DOMAIN\username

Enhancements to the Xerox® Workplace Suite server, allow the matching of the UPN value to the DOMAIN\username value, so that the user may be presented with their list of jobs and release them from the Printer Client (EIP App).

Printer Client Release Permissions

The Printer Client (or EIP App) provides an interface on some Xerox devices to view and release the user’s printer jobs. This includes both Mobile Print jobs and Print Management Workflow submitted jobs. By default, only the user that submitted a job will be allowed to view and manage their jobs. However, the Xerox® Workplace Suite system allows users to grant access permission to other users in the system to view and manage their jobs. This feature is available when the User Portal interface has been enabled.

Company > Policies > Security > User Portal

Once enabled, users may log into the web portal:

https://<server>/login

After logging into the web portal, users have access to the Delegation tab, allowing them to both view the list of users which have granted them permission to access their print jobs using the “Print Theirs” tab. They may also grant permission to other user users to access their print jobs. Details on this functionality can be found in the administration guide for this solution.

Release permissions are only supported via the Printer Client. This configuration does not impact any other interface (e.g., Workplace App). Users can always view the list of users that have been granted release permission to their documents and they may revoke that ability at any time.

To help distinguish who is releasing a job versus who originally sent it, the job history (Jobs > History) and reports (Reports > Job Reporting) summary have been updated for the CSV export capability to include “Printed By Email” and “Print By User Name” fields. These fields are populated with corresponding information from the person that released the job to the printer using the Printer Client.

Administration Recovery

The Administration Recovery Procedure is used to log in to repair settings that prevent you or another

Administrator from logging in. This procedure allows you to assign a new Administrator, repair email, LDAP, and other settings. When using this feature, the User Portal authentication mechanism is reset to “Email and Confirmation Number”. If this is not the preferred login method, change the User Portal authentication method back to your desired configuration. To access the Administration Recovery Procedure, you must use Domain or Workstation local user account the satisfiessatisfies either of the following requirements:

- The User must be in the “Administrator” group of the server.
- The User must be in the “MPAdmin” group of the server

Details on using the feature can be found in the Administration and Configuration Guide.

Single Sign-On

The SSO capability was designed with a focus on security of the Gallery App authentication data (credentials, token, etc.). Below is a highlight of the main security points of this solution:

- All communication is over HTTPS.
- The WS server validates the certificate of the App Server vault. The certificate must be from a well-known and trusted provider, or it must exist in the trusted root certs on the server (e.g., if generated from a local certificate authority).
- The SSO authentication data for a given user and app is given to the WS Server in an encrypted format. The WS can never view the authentication data. [Note: It is the responsibility of the App from the Gallery and/or its backend server to encrypt the authentication data before sending it to WS for storage].
- Exchange of sensitive information between WS and the App / App Server uses public key cryptography with asymmetric keys. Each side (WS and App Server) has its own public and

private keys, and shares the public key with the opposite side, but keeps its private key hidden. Data is encrypted by the public key and then sent to the owner of the private key to decrypt it.

- All message exchanges related to authentication data include digital signatures, so that the receiver can always validate that the request is coming from a trusted entity.
- Messages containing authentication data include 3 levels of encryption:
 - The channel is encrypted via HTTPS.
 - Message content is encrypted using public key cryptography with asymmetric keys. An RSA algorithm is used for encryption with a key size maximum of 16384.
 - Authentication data is encrypted by the Gallery App or its backend server prior to storing it with WS. The format and encryption method used are up to the Gallery APP vault.

Data sent from one entity to the other is always encrypted using the public key of the receiver. As an example, let's assume the App / Gallery App Server would like to store new authentication data on the WS Server. The steps to manage the encryption of this data are as follows:

1. The Gallery App Server constructs the appropriate message data to be sent to WS, and then encrypts that data using the public key of WS.
2. That data is then signed by the App Server using its own private key.
3. When this data is received by WS, it validates the signature using the public key of the Gallery App Server.
4. The message is then decrypted by WS using its private key.

A similar exchange takes place when sending the response message from the SSO vault to the Gallery App Server.

8. Additional Information and Resources

Security @ Xerox

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see <https://www.xerox.com/security>.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: <https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html>.

Additional Resources

Below are additional resources.

Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/



Xerox and Information Security

Your Data, Your Business:
Partnering to Protect What's
Most Important



Table of Contents

- 1 Overview 3
- 2 Security Vulnerabilities: Industry Risks and Costs 5
- 3 Security Overview 7
- 4 Regulatory and Policy Compliance 19
- 5 Risk Assessment and Mitigation 20
- 6 Manufacturing and Supplier Security Practices. 21
- 7 Product Returns and Disposals 22
- 8 Summary 23
- 9 Security Checklist 24

Overview

Information is every organization's key asset, and security is essential to the office—for documents and for any devices, including printers and multifunction printers, connected to the network. And in the 21st century, the network is the hub of virtually all business activity.

Nearly every business, and every person in it, is connected to the Internet. Your business—and every organization with which you collaborate—is part of a global system of interconnected computer networks and servers. There are countless users simultaneously performing tasks, accessing and sharing information, shopping for and selling goods and services and communicating via email, instant messaging, Skype™, Twitter and many other services.

The security threat is very real and the stakes are growing at exponential rates. A breach in the security of an organization's documents can result in unauthorized acquisition or use of sensitive or proprietary information. It can lead to harmful disclosure, stolen or compromised intellectual property and trade secrets. And for many organizations, these security breaches can end with costly fines and litigation, to the tune of hundreds of thousands to millions of dollars.

Today's rising security threats come in various forms and in varying degrees of severity. The explosive proliferation of networked devices means an ever-increasing number of potentially vulnerable points of entry for intruders. And the "hacker" threat is constant, with programs running 24/7 that automatically seek and exploit network security shortcomings.

Security threats vary from relatively harmless spam messages to persistent threats that can take down entire networks.

With such constant Internet activity, you must be sure your company's confidential information stays secure. But the demands change, and change daily.

Networked printers and multifunction printers, or MFPs, which can print, copy, scan to network destinations, send email attachments and handle incoming and outgoing fax transmissions, are particularly vulnerable.

For those in Information Security, it's critical to the security of an organization's network to make sure that security infractions can't happen through network-connected printers and MFPs—or at the devices themselves. After all, attacks can originate in unexpected ways:

- The phone line attached to an MFP could be used to access the network.
- The Web server used to manage the MFPs and printers may be vulnerable to attack.
- Unprotected electronic data can be inappropriately accessed while at rest on the hard disk or in motion to/from the device.
- Malicious emails can be sent from an MFP with no audit trail.

Printers and multifunction printers are sophisticated, multiple sub-system IT platforms, and meaningful security measures must comprehend every element of the platform.

Today's printers and MFPs are quite different from PCs and servers.

- Printers and MFPs are shared devices with multiple users and multiple administrators.
- Printers and MFPs are embedded devices:
 - There may be a real operating system within the system.
 - The operating system may have a direct external interface.
 - The operating system may be proprietary.
 - The operating system may be Microsoft® Windows®.
- Printers and MFPs have the following, all of which are typically associated with more advanced computing nodes:
 - Network protocol stacks
 - Authentication and authorization functions
 - Encryption
 - Device management
 - Web servers

Overview

Heterogeneity of printer and MFP implementations poses challenges.

- Much more diverse than traditional PCs
- High degree of diversity regarding underlying operating systems among different manufacturers and even within single manufacturer product lines

Traditional PC and server controls are not optimized for printers and MFPs.

- Anti-virus approach
 - May not be available for the operating system type used in the printer and MFP
 - Generally losing the war against malware anyway
 - Complexity of managing data file updates in a distributed environment
- Patching printers and MFPs
 - Software version control of printers and MFPs is inconsistent
 - Configuration management creates operational overhead
- Security Information and Event Management (SIEM)
 - Alerts and awareness from printers and MFPs are uneven
 - Remediation of printers and MFPs is not standardized

This is a very different situation from the printers and copiers of yesterday.

Just about anyone can launch attacks against a network and a company's information assets if a printer and MFP's physical and electronic access isn't securely controlled and protected. Those attacks can be as simple as someone picking up documents left in the printer and MFP's output tray to malicious worms pulling sensitive documents off the network.

A printer's and MFP's entire system, along with any device management software on the network, must be evaluated and certified so that Information Security and all the workers of an organization are certain that their documents and network are safe and secure from information predators—or even from internal security breaches.

In that respect, not all printers and MFPs are equal. Therefore, a comprehensive approach, based on foundational, functional, advanced and usable security, is critical to safeguarding the information assets of today's businesses.

Thankfully, Xerox has the security capabilities to help. For the last 20 years, Xerox has been a leader in providing secure document solutions to a variety of industries across the globe. In fact, every Xerox® product and service we offer was designed with security in mind and to seamlessly integrate into existing security frameworks. Plus, security is managed throughout the entire product life cycle from requirements analysis, design, development, manufacturing, deployment and disposal—giving you and your customers more protection and peace of mind.

At Xerox, we help protect your data at every potential point of vulnerability so you don't have to. By staying focused on what we do best, you can stay focused on what you do best.

Xerox Security Goals

We've identified five key security goals in our quest to provide secure solutions to every one of our customers:

CONFIDENTIALITY

- No unauthorized disclosure of data during processing, transmission or storage

INTEGRITY

- No unauthorized alteration of data
- System performs as intended, free from unauthorized manipulation

AVAILABILITY

- System works properly
- No denial of service for authorized users
- Protection against unauthorized use of the system

ACCOUNTABILITY

- Actions of an entity can be traced directly to that entity

NON-REPUDIATION

- Mutual assurance that the authenticity and integrity of network communications are maintained

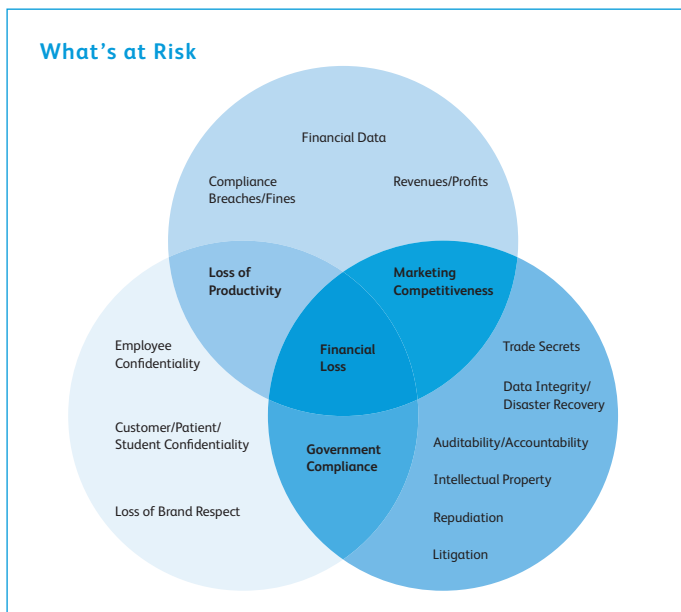
Security Vulnerabilities: Industry Risks and Costs

Businesses of all sizes have sensitive information valuable to cybercriminals that must be protected. The threat landscape is changing constantly. With an increase in Bring Your Own Devices (BYOD), wearables for health-tracking data, mobile payment systems, cloud storage and the Internet of Things, the threat is real and continues to grow.

Cybercriminals are increasingly focusing their attention on small- and mid-sized businesses (SMBs), because they are easier targets than large enterprises and because SMBs typically lack the resources needed to protect themselves against attacks. Data breaches for large enterprises make news headlines but, unfortunately, we don't hear much in the news about cyber-attacks on SMBs.

The stakes for SMBs are even higher than for large corporations. Customer information maintained within SMBs is becoming a more valuable commodity and the costs of these breaches can devastate an SMB. According to a study conducted in 2015 by IBM and Ponemon Institute, the average total cost of a data breach for the participating companies increased 23% over two years to \$3.79 million.¹ The average cost paid for each lost or stolen record containing sensitive and confidential information increased from \$145 in 2014 to \$154 in 2015.¹

That doesn't account for possible fines, loss of reputation and business disruption. Security may not always be a top business priority, but keeping information protected is critical for the health of the organization.



Healthcare

Advances in information technology—including the use of handheld computers—have created the need to share important medical data and patient information electronically—and that's where security becomes a major concern.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was put in place by the federal government to force all healthcare organizations to apply uniform data management practices to protect patient information and patient privacy at all times. Under HIPAA, an audit trail is required to track who viewed data, when they viewed it and if they had the proper authorization to do so.

The Health Information Technology for Economic and Clinical Health (HITECH) Act significantly expanded the U.S. government's efforts to establish a national electronic record keeping system for the healthcare industry. HITECH was enacted as part of the American Recovery and Reinvestment Act of 2009 to promote the adoption and meaningful use of health information technology.

Failure to comply with HIPAA can result in civil and criminal penalties, even if no breach occurs.

Government

Today, local, state and federal governments have put an emphasis on simplifying processes and improving cross-agency collaboration to provide better outcomes for the citizens they serve. To do so, they're employing various initiatives to take advantage of the latest technologies, while putting strict regulations in place to ensure the information being shared is safe and secure. One example is the Massachusetts state data breach law, which is one of the most aggressive in the nation. Xerox® systems, software and services conform to these strict guidelines, as well as others.

In 2014, the Department of Defense adopted National Institute of Standards and Technology (NIST) 800-53 standards, which is a publication that recommends security controls for federal information systems and organizations, and document security controls for all federal information systems, except those designed for national security.

1. 2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.

Security Vulnerabilities: Industry Risks and Costs

Also, the Department of Defense has adopted additional security measures with the use of Common Access Cards (CAC) and their civilian government counterparts, Personal Identity Verification (PIV) cards. Such cards require a PKI infrastructure to ensure a secure authentication and communications environment. Additionally, most federal government agencies have adopted the FIPS 140-2 standard to certify encryption modules used in printer and MFP products. And finally, many federal government customers require products be certified to the Common Criteria standard.

Financial Services

Direct deposit, online banking, debit cards and other advances in information technology are revolutionizing the financial services industry. Though more convenient for both customers and businesses, this heavy use of technology has its own set of security concerns.

A secure exchange of credit card information is vital and compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) helps to alleviate vulnerabilities and protect cardholder data. PCI DSS is a proprietary information security standard for organizations that handle credit cards, including Visa®, Mastercard®, American Express®, Discover® and JCB.

The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA) was instituted to ensure financial institutions that collect or receive private customer data have a security plan in place to protect it. To reach compliance, organizations must complete a risk analysis on their current processes and implement firewalls, restrict user access, monitor printing and more.

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 further increases the need for accurate collection and reporting of financial data. Through the Office of Financial Research and member agencies, data will be collected and analyzed to identify and monitor emerging risks to the economy and make this information public in periodic reports and annual testimony to Congress.

Education

With today's educational institutions—including K–12, colleges and universities—transcript requests, financial aid applications and even class notes can all be found online. Because some schools have their own medical centers, they also have to store and share medical information electronically. This interactive environment enhances the student experience and improves staff productivity, but it also makes schools susceptible to security threats.

Because these institutions manage a variety of information, many state and federal regulations apply, including the Computer Fraud and Abuse Act, USA Patriot Act, HIPAA and GLBA. However, the most applicable regulation to the education industry is the Family Education Rights and Privacy Act (FERPA). This act prohibits the disclosure of personally identifiable education information without the written permission of the student or the student's guardian.

With so many regulatory and compliance measures requiring a response, Xerox has looked to the federal government requirements, among others, as guidelines. By developing solutions that strive to meet the most stringent security standards, we can offer highly secure solutions to all of our customers—regardless of business sector.

Security Overview

At Xerox, our “Security = Safety” philosophy drives the development of products, services and technologies that are infused with security at every level.

Security is front and center when engineering our “Smart MFPs.” As a leader in the development of digital technology, Xerox has demonstrated a commitment to keeping digital information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Customers have responded by looking to Xerox as a trusted provider of secure solutions that offer a host of standard and optional state-of-the-art security features.

Our Security Strategy

The development of Xerox® products is guided by a Secure Development Life Cycle Process, which takes the Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM) and SANS Institute guidelines into consideration. This involves defining security requirements, assessing risks, analyzing vulnerabilities and penetration testing, as well as information obtained from OWASP and the SANS Institute. This strategy consists of three pillars:

State-of-the-Art Security Features

Printers and multifunction devices are sophisticated, multiple sub-system network platforms, and Xerox offers the broadest range of security functionality on the market, including encryption, authentication, authorization per user and auditing.

Certification

ISO 15408 Common Criteria for Information Technology Security Evaluation is the only internationally recognized standard for security certification. Xerox was the first manufacturer to seek and obtain certifications for “complete” MFP devices. Because each element of the multifunction platform is a potential point of entry, meaningful security certification must comprehend all elements, including the operating systems, network interface, disk drive(s), Web server, PDL interpreter(s), MFP user interface, local hardware ports and fax system.

Maintenance

At Xerox, maintaining our printer and multifunction devices’ security throughout their lifespan requires ongoing diligence to ensure continuous protection against newly discovered exploits. This is accomplished by:

- Ensuring that software updates are issued on an ongoing basis
- Notification of new security bulletins with RSS feeds
- Responding to identified vulnerabilities
- Providing secure installation and operation guidelines
- Providing Common Criteria information
- Making patches available at www.xerox.com/security

The Xerox Security Model, in concert with the Secure Development Life Cycle, is a commitment that all features and functions of the system, not just one or two, are safe and secure.

Security Overview

A Comprehensive Approach to Printer and MFP Security

Xerox long ago recognized and embraced this shift in technology and the evolving needs of the workplace. We offer a comprehensive set of security features to keep your printers/MFPs and your data safe. Xerox secures every part of the data chain, including print, copy, scan, fax, file downloads and system software. **There are four key aspects to our multilayered approach.**

1. Intrusion Prevention

Your first and most obvious vulnerability is the user interface—who has physical access to your printer and its features. User Authentication is the basis for granting access to Xerox® printers and multifunction devices for authorized walkup and network users. Once authenticated, the user can interact with the device or access customer data, which is subject to restrictions based on the user's role. Xerox® printers and MFPs employ a variety of technologies to ensure authorized access to device features and functions by users and other network devices. Then we tackle less obvious points of intrusion—what is sent to the printer and how Xerox® ConnectKey® Technology will intercept attacks from corrupted files and malicious software. Our system software, including DLMs and weblinks, is Digitally Signed: any attempts to install infected, non-signed versions will result in the file being automatically rejected. Print files will also get deleted if any part is not recognized as legitimate.

NETWORK AUTHENTICATION

Network authentication allows users to authenticate to the device by validating user names and passwords prior to use. Network authentication authorizes an individual to access one or any combination of the following services: Print, Copy, Fax, Server Fax, Reprint Saved Jobs, Email, Internet Fax and Workflow Scanning Server. Also, users can be authorized to access one or any combination of the following machine pathways: Services, Job Status or Machine Status.



1. Intrusion Prevention

Prevent general access to restricted devices with user access and internal firewall on the printer.



2. Device Detection

Be alerted at startup or on demand if any harmful changes to your printer have been detected.



3. Document and Data Protection

Keep personal and confidential information safe with encrypted hard disk (AES 256-bit, FIPS validated for many products) and image overwrite.



4. External Partnerships

Protect your data and device from malicious intrusions with McAfee whitelisting technology, Cisco® Identity Services Engine (ISE) integration, certification bodies and compliance testing organizations.

MICROSOFT® ACTIVE DIRECTORY® SERVICES

The Microsoft Active Directory Services (ADS) feature enables the device to authenticate user accounts against a centralized user account database, instead of exclusively using the user account database that is managed locally at the device.

LDAP AUTHENTICATION

LDAP authentication (BIND) is supported for authenticating with the LDAP servers for information lookup and access. When an LDAP client connects to the server, the default authentication state of the session is set to anonymous. The BIND operation establishes the authentication state for a session.

SMTP AUTHENTICATION

This feature validates the user's email account and prevents unauthorized users from sending emails from the device. System Administrators can enable TLS for all SMTP send and receive operations.

Security Overview

POP3 AUTHENTICATION BEFORE SMTP

As an additional layer of security, Xerox® MFPs support the ability for System Administrators to enable or disable the POP3 authentication before SMTP feature. POP3 authentication before SMTP forces a successful login to a POP3 server prior to being able to send mail via SMTP.

ROLE BASED ACCESS CONTROL (RBAC)

The RBAC feature ensures that authenticated users are assigned to a role of either Non-logged-in User/Logged-in User, System Administrator or Accounting Administrator. Each role has associated privileges with appropriate levels of access to features, jobs and print queue attributes. It enables Administrators to choose precisely which functions are permitted for a given role. Once a user logs into the device with the user's name and password, the device can determine which roles are assigned to that particular user. Restrictions are applied based on the assigned roles. If an entire function is restricted, it can appear locked out to the user after authentication or not appear at all.

Non-logged-in User/Logged-in User System Administrator Accounting Administrator

PRINT USER PERMISSIONS

Xerox user permissions provide the ability to restrict access to print features by user, by group, by time of day and by application. Users and groups can be set up with varying levels of access to print features. For example, limits can be set that allow color print jobs only during certain hours of the day; Microsoft® PowerPoint® presentations automatically print in duplex mode; or Microsoft Outlook® emails always print in black and white.

Feature	Name	Print Submitter Unknown
Time	Black & White Printing	
Time	Color Printing	
Simplex	1-Sided Printing	
Paper Tray	Tray 1	
Paper Tray	Tray 2	
Paper Tray	Tray 3	
Paper Tray	Tray 4	
Paper Tray	Tray 5 (Bypass)	
Job Type	Secure Print	
Job Type	Normal Print	
Job Type	Sample Set	

Set color user permissions and other print restrictions with intuitive graphical interfaces.

SMART CARD AUTHENTICATION

Also known as Proximity Card or Contactless Smart Card Authentication, Smart Card Authentication protects your printer and MFP from unauthorized walkup access. Xerox® devices support multiple major smart cards (CAC/PIV, .NET, Rijkspas and other smart and proximity cards), around 30 different types of card readers and 65 different proximity cards. With Smart Card Authentication, users can be authenticated using a two-factor identification system—possession of the card and a personal identification number entered at the device's user interface—to gain access to the walkup features at the device and on the network.



The Common Access Card/Personal Identity Verification (CAC/PIV) is a U.S. Department of Defense smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-government employees and eligible contractor personnel. The CAC/PIV can be used for general identification, controlled building access and for authentication of personal computers, in addition to printers/MFPs and the networks that connect them.

Security Overview

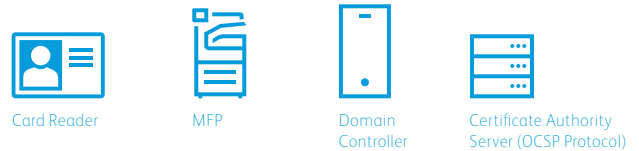


The 144k CAC/PIV is a version of the smart card. Users can be authenticated using two-factor identification to gain access to walkup services at the device.

The 144k CAC/PIV provides the following benefits:

- Scan to Email S/MIME encryption to self or any recipient in the MFP's local or LDAP global address book
- Digital signing using the Email Signing Certificate from the user's card
- Automatic population of the "To:" field when using the MFP's Scan to Email function
- Up to 2048-bit certificate key
- Restrict outgoing transmissions to recipients with valid certificates
- Receive email confirmation reports and maintain audit logs
- Single signon to Scan to Home and LDAP

Configuration Diagram for Common Access Card (CAC)/ Personal Identity Verification (PIV)

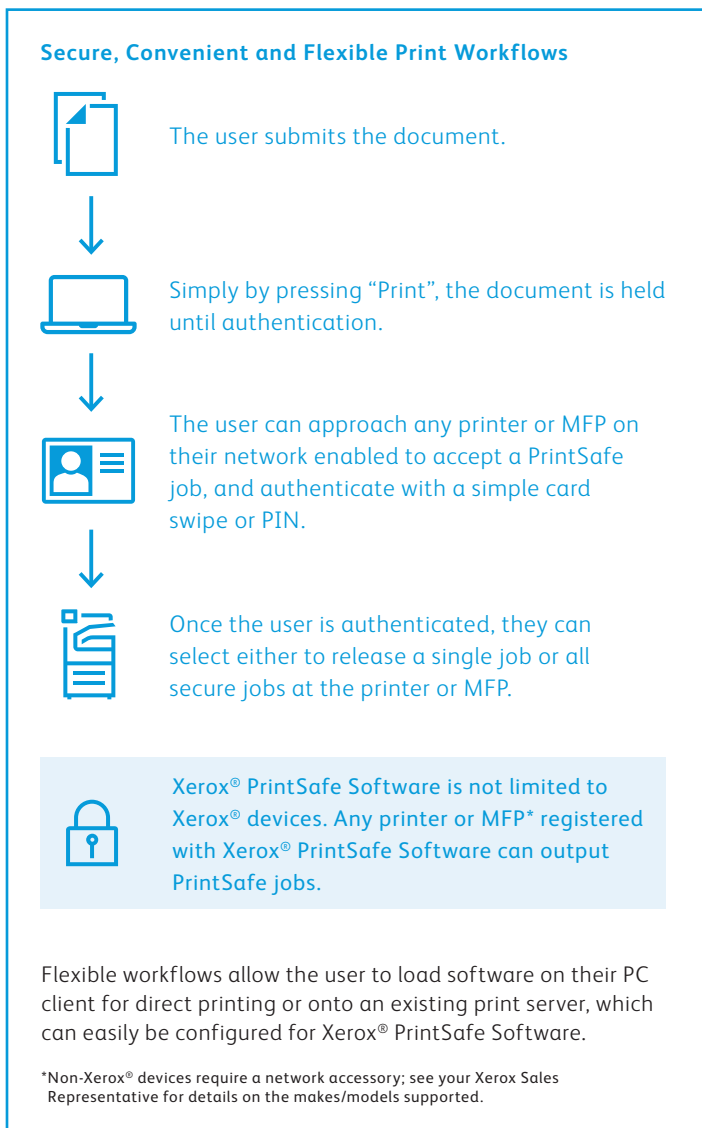


1. A card is inserted into the reader and the user is prompted to enter a PIN at the MFP.
2. The MFP checks the OCSP server to confirm that the card's certificate has not expired and then verifies the "Chain of Trust" back to a known Certificate Authority.
3. The MFP initiates an encrypted challenge/response dialog between the Domain Controller and the Common Access Card. If successful, the Domain Controller issues a "Ticket Granting Ticket" and authorization is complete.
4. Authorization unlocks Walkup MFP features:
 - Scan to Email
 - Copy
 - Fax
 - Custom Services
 - Workflow Scanning

Security Overview

XEROX® PRINTSAFE SOFTWARE

Xerox® PrintSafe Software provides secure print authentication for printed data on most printers and MFPs, including both Xerox® devices and devices from other vendors. This software is open to work with a variety of industry standard secure readers and cards.



DEVICE USER INTERFACE AND REMOTE USER INTERFACE ACCESS

System Administrators can lock out access to device setup screens for unauthorized users from the control panel and Remote User Interface utility in an effort to protect its configuration information.

2. Device Detection

In the unlikely event that your data and network defenses are bypassed, Xerox® ConnectKey® Technology will run a comprehensive Firmware Verification test, either at start-up* or when activated by authorized users. This alerts you if any harmful changes to your printer or MFP have been detected. If any anomalies are detected, the device will display a message advising the user to reload the firmware. Our most advanced built-in solutions use McAfee® Whitelisting** technology that constantly monitors for and automatically prevents any malicious malware from running.

In partnership with Cisco, Xerox has implemented our device profiling in Cisco® Identity Services Engine (ISE). Integration with Cisco Identity Services Engine (ISE) auto-detects Xerox® devices on the network and classifies them as printers for security policy implementation and compliance.

For more information, refer to the following white papers:

McAfee Whitelisting White Paper:

<http://www.office.xerox.com/latest/SECWP-03.PDF>

Cisco ISE White Paper:

<http://www.office.xerox.com/latest/SECWP-04.PDF>

*Xerox® VersaLink® Printers and Multifunction Printers

**Xerox® AltaLink® and i-Series Multifunction Printers

Security Overview

3. Document and Data Protection

Document Protection

Even when all necessary network security measures are in place to effectively protect critical data as it travels between users' computers and office printing devices, security technologies must also ensure that your sensitive hard-copy documents are received and viewed only by their intended recipients. Xerox employs the latest technologies to safeguard your output, whether printing hard copies or distributing electronic documents.

SCAN DATA ENCRYPTION

Users of our Xerox® ConnectKey® Technology-enabled i-Series, VersaLink® and AltaLink® Series Smart MFPs also have the option to encrypt PDF files with a password when using the Scan to Email service.

- Protection outside of firewall
 - Securing data in an unsecure environment
 - Using industry standard protocols such as TLS and Secure PDF

PRINT STREAM ENCRYPTION

The Xerox® Global Print Driver® and some product drivers support document encryption when submitting Secure Print print jobs to ConnectKey Technology-enabled devices. Xerox® AltaLink and i-Series Multifunction Printers also support document encryption for regular print jobs. No additional hardware is required for print driver encryption.

SECURE PRINT

Sensitive print jobs are held at the printer or MFP until the document owner releases them by entering their unique PIN through the device's user interface. This ensures that a document's intended recipient is physically present when printing sensitive information and can immediately remove the output from the printer or MFP before exposing it to other device users.



Secure printing based on Common Access Card (CAC)/Personal Identity Verification (PIV) card technologies attaches the print-job sender's identity certificate to their print job. At the device, the user must authenticate with the user's CAC/PIV card before the job will be released.

ENCRYPTED PDF/PASSWORD-PROTECTED PDF

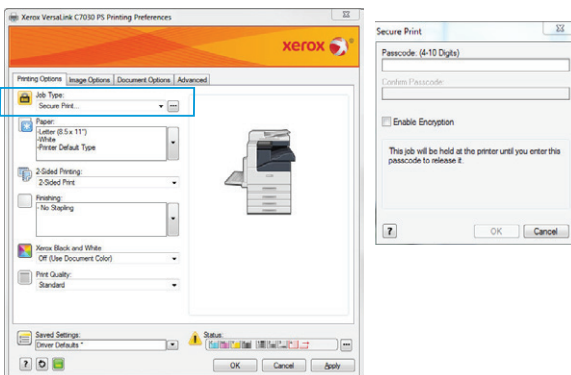
When scanning a hard-copy document for electronic distribution via the Scan to Email feature, Xerox® MFPs can create 128-bit or 256-bit AES-encrypted PDFs or password-protected PDFs, which are then securely transmitted over the network, and can be opened, printed or changed only by those who possess the correct password.

FAX FORWARDING TO EMAIL AND NETWORK

Xerox® MFPs with fax forwarding capability can route incoming faxes to specific recipients' email in-boxes and/or to a secure network repository, where they can be accessed only by authorized viewers.

FAX DESTINATION CONFIRMATION

A fax sender receives automated confirmation that the sender's fax was successfully received by the intended recipient.



Security Overview

DIGITAL SIGNATURES

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A digital signature is used to protect the device firmware from undetected modification and to provide data origin authentication. With smart cards, emails can be digitally signed with the sender's certificate. A valid digital signature gives the recipient confidence to believe that the message was created by a known sender and that it was not altered in transit.

SECURE WATERMARKS

Some Xerox® printers and MFPs have a Secure Watermark feature that helps prevent original printouts with sensitive information from being copied. If a document with a secure watermark is copied, the watermark image becomes visible, making it apparent that the document contains sensitive information and has been illegally duplicated.

USER/TIME/DATE STAMP

Through the Xerox® drivers, a user/time/date stamp can be applied to any document printed by any networked device. This provides an audit trail of who printed what, and at what time.

IP ADDRESS FILTERING

Internet Protocol (IP) filtering allows System Administrators to create rules to accept or reject information coming to the MFP device based on specific IP addresses or range of addresses. This gives the System Administrator control over who can and cannot access the device.



Registered IP Addresses:
Available



Non-Registered IP Addresses:
Not Available

SECURE SOCKETS LAYER (SSL)/TRANSPORT LAYER SECURITY (TLS)

Many organizations are required to comply with security policies that require all transactions between the client and printer or MFP to be secure via secure Web transactions, secure file transfers and secure emails. Data that is transmitted over the network without encryption can be read by anyone that sniffs the network. Xerox mitigates this problem with Secure Sockets Layer/Transport Layer Security for transmissions of data over certain protocols such as HTTPs and IPP.

IPSEC ENCRYPTION

Internet Protocol Security (IPsec) secures all communication at the IP layer and is primarily used to encrypt print submittals to the device. It encrypts all traffic between Point A and Point B in such a way that only trusted users can send and receive the information, the data is not altered during its transmission and only authorized users can receive and read the information.

IPsec is designed to provide the following security services:

- Traffic encryption (preventing unintended parties from reading private communications)
- Integrity validation (ensuring traffic has not been modified along its path)
- Peer authentication (ensuring that traffic is from a trusted party)
- Anti-replay (protecting against replay of the secure session)

NETWORK PORTS ENABLE/DISABLE

With the Network Ports Enable/Disable capability, unnecessary ports and services can be disabled to prevent unauthorized or malicious access. On smaller desktop devices, these options can be adjusted through their control panel or PC-based configuration software. On larger MFPs, tools are provided to set security levels and disable specific ports and services.

Security Overview

DIGITAL CERTIFICATES

Digital certificates are electronic documents that use a digital signature to bind a public key with an identity—information such as the name of a person or an organization, their address and so forth. The certificate can be used to verify that a public key belongs to an individual.

MFPs can add digital signatures that verify the source and authenticity of a PDF document. When recipients open a PDF file that has been saved with a digital signature, they can view the document's properties to review the signature's contents including the Certificate Authority, system product name, serial number and the time/date stamp of when it was created. If the signature is a device signature, it will also contain the name of the device that created the document, while a user signature verifies the identity of the authenticated user that sent or saved the document.

Xerox® MFPs can be loaded with a certificate signed by a certificate authority such as VeriSign, or your System Administrator can create a self-signed certificate on the device itself. By setting up a certificate on your device, you can enable encryption for specific types of workflows.

SNMPV3

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks, which provides greater security by protecting data against tampering, ensuring access is limited to authorized users through authentication and encrypting data sent over a network.

Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). The SNMPv3 protocol provides significantly enhanced security functions including message encryption and authentication.

SNMP COMMUNITY NAME STRINGS

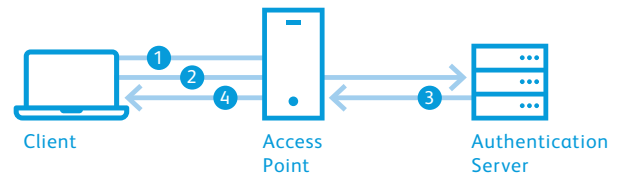
Typical read-only Management Information Base (MIB) data use the "public" string and the read-write community strings that are set to "private." Using the read-write community name strings, an application can change the configurations setting of the device using MIB variables. The read-write community name strings on Xerox® devices can be changed by the System Administrator to increase the security when managing MFPs using SNMP.

802.1X AUTHENTICATION

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a local area network (LAN) or wireless local area network (WLAN). IEEE 802.1X functionality is supported by many Ethernet switches and can prevent guest, rogue or unmanaged systems that cannot perform a successful authentication from connecting to your network.

How It Works: 802.1X Authentication

802.1X authentication for wireless LANs provides centralized, server-based authentication of end users.



1. A client sends a "start" message to an access point, which requests the identity of the client.
2. The client replies with a response packet containing an identity, and the access point forwards the packet to an authentication server.
3. The authentication server sends an "accept" packet to the access point.
4. The access point places the client port in authorized state, and traffic is allowed to proceed.

Security Overview

The 802.1X protocol has become more prevalent with the increased popularity of wireless networks. Many organizations lock down port access to their internal networks using this protocol. This prevents any information from passing onto the network until the device is authenticated. From a risk management perspective, this allows for both wireless and wired devices to prove who they are before any information is passed through to the network. If unauthorized access is attempted, the port is locked down until unlocked by the System Administrator.

The Extensible Authentication Protocol (EAP) is an authentication framework that performs its functions as part of 802.1X authentication. EAP types currently supported by Xerox® MFPs are:

- EAP-MD5
- PEAPv0/EAP-MS-CHAPv2
- EAP-MS-CHAPv2
- EAP-TLS (AltaLink® and i-Series products)

FIREWALL

A firewall is a part of a computer system or network that is designed to block the device from external threats and unauthorized access while permitting authorized communications. The device can be configured to permit or deny network transmissions based upon a set of rules and other criteria. Network Administrators can restrict access to network segments, services and the devices' ports to secure the devices.

FAX AND NETWORK SEPARATION

Separating the fax interface from the network controller eliminates the security risk of hacking into an office network via the fax line.

The MFP does not provide a function to access the network via the fax phone line. The Fax Class 1 protocol used on the MFP only responds to fax commands that allow the exchange of fax data. The data passed from the client PC can only be compressed image data with destination information. Any data other than image information (such as a virus, security code or a control code that directly accesses the network) is abandoned at this stage, and the MFP immediately ends the call. Thus, there is no mechanism by which to access the network subsystem via the fax line.

Data Protection

Technology has transformed the way employees conduct business. Today, documents take shape in not only the traditional hard copy forms, including handwritten notes and draft versions of paper communications, but also in electronic forms on desktops and in email. Because employees create, store, share and distribute these electronic documents differently than traditional paper documents, this information may be subject to new types of risks. To remain competitive, a company must address these threats by securing the documents and document management systems that contain a company's most valuable asset—knowledge.

Information and document management systems face a wide range of security threats. These threats include intentional espionage acts, such as computer hacking, theft, fraud and sabotage, as well as unintentional acts such as human error and natural disasters. Information security is more than protection. It is about ensuring timely access and availability of document content to improve business process and performance. It is also about managing original content and complying with federal regulations.

From the introduction of the first digital products, Xerox has recognized the risk of retained data being inappropriately recovered from non-volatile storage and built features and countermeasures into our devices to help customers safeguard their data.

IMAGE DATA ENCRYPTION

Using 128-bit or 256-bit AES encryption, many Xerox® devices feature data encryption including job, image and customer data, which protects your Xerox® MFP's data at rest from unauthorized access. With data encryption, the disk is partitioned and only the user data partition is encrypted. Operating system partitions are not and cannot be encrypted.

- AES 128-bit or 256-bit encryption, Federal Information Processing Standard (FIPS) 140-2 validated
- All user image data on the hard disk is encrypted

Security Overview

AES is a small, fast, hard-to-crack encryption standard and is suitable for a wide range of devices or applications. It is the state-of-the-art combination of security, performance, efficiency, ease of implementation and flexibility. Many Xerox® devices can be put into FIPS 140-2 mode, which means that they will utilize only FIPS 140-2 certified encryption algorithms.



IMAGE OVERWRITE

Image overwrite erases image data from your Xerox® device's hard drive once the data is no longer needed. This can be performed automatically after completion of processing each job, scheduled on a periodic basis, as well as at the request of the System Administrator. Xerox® devices feature both Immediate and On Demand Image Overwrite.



VOLATILE AND NON-VOLATILE MEMORY

Within every Xerox® MFP, the controller includes volatile memory (RAM) and non-volatile memory (hard disk). With volatile memory, all image data is lost upon shutdown or system reboot. With non-volatile memory, image data typically is stored either in flash or on the MFP's hard drive, and is preserved until it is erased.

As concerns for data security increase, customers want to know how and where data can be compromised. Statements of Volatility are documents created to help identify where customer image data is located in Xerox® devices. A Statement of Volatility describes the locations, capacities and contents of volatile and non-volatile memory devices within a given Xerox® device.

Statements of Volatility have been created for many Xerox® devices to help security-conscious customers. These documents may be obtained by contacting your local Xerox support team (for existing customers), a Xerox sales professional (for new customers) or may be accessed at www.xerox.com/security.

SECURE FAX

Sensitive incoming faxes are held until released by the System Administrator.

SCAN TO MAILBOX PASSWORD PROTECTION

When using an MFP's Scan to Mailbox feature, the designated mailbox can be password protected to ensure only those authorized can access the scans stored within it. Scan to Mailbox security is further enhanced by encryption of the hard disk image data partition.

S/MIME FOR SCAN TO EMAIL

Secure/Multipurpose Internet Mail Extensions (S/MIME) provides the following cryptographic security services for the Scan to Email feature: authentication, message integrity and non-repudiation of origin (using digital signatures), and privacy and data security (using encryption).

In S/MIME communication, when sending data to the network, a signature is added to each mail message based on the certificate information retained in the device. Encryption is performed when sending data based on the certificate corresponding to each mail message's designated address. The certificate is verified when data transmission information is entered, as well as when the data is to be sent. S/MIME communication is conducted only when the certificate's validity is confirmed.

SCAN TO EMAIL ENCRYPTION

Email encryption via Smart Card Authentication allows users to send up to 100 encrypted emails to multiple recipients in an organization's LDAP directory using the recipients' public keys. Most Xerox® MFPs using Smart Card Authentication also provide the ability to digitally sign emails. Users may view certificates of potential recipients prior to sending email. The MFP disallows sending to users without an encryption certificate. Also, the MFP logs all records of email sent with an option for the administrator to receive confirmation reports.

JOB LOG CONCEAL

The standard Job Log Conceal function ensures that jobs processed through the device are not visible to a walkup user or through the Remote User Interface. The Job Log information, although concealed, is still accessible by the System Administrator, who can print the Job Log to show copy, fax, print and scan usage on the device.

Security Overview

HARD DRIVE RETENTION OFFERING

Xerox provides a Hard Drive Retention Offering for Xerox® devices to those customers who are concerned that the image data on their hard drive is more sensitive or even classified. This service allows a customer, for a fee, to retain their hard drive(s) and sanitize or destroy them in a manner that they feel will keep their image data secure.

REMOTE SERVICES DATA VALIDATION

Many Xerox® devices obtain customer buy-in prior to transmitting Personal Identifiable Information (PII) and Customer Identifiable Information (CII) via Remote Services to Xerox.

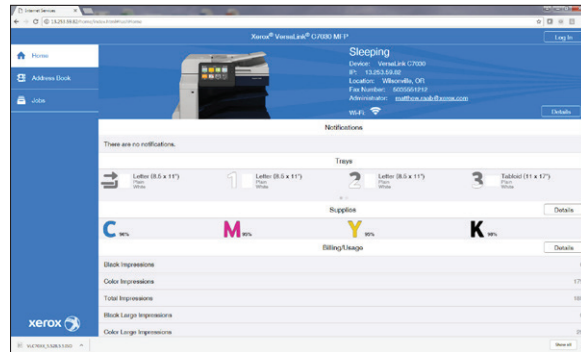
POSTSCRIPT PASSWORDS

Another printing-related area of risk is when printing with the Adobe® PostScript® page description language (PDL). PostScript includes commands that allow print jobs to change the device's default behaviors, which could expose the device. Because the PostScript language includes very powerful utilities that could be used to compromise a device's security, administrators can configure the device so that PostScript jobs are required to include a password to change the device's default behaviors. The basic privileges of the PostScript interpreter within the controller are limited by design, but administrators have some capability to manage the operation of the PostScript subsystem.

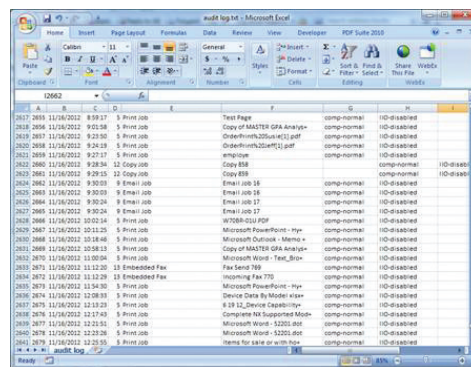
AUDIT LOG

Xerox® MFPs and many of our printers can maintain Audit Logs to track activity by document, user and function. The Audit Log is enabled by default on newer devices and can be enabled or disabled by the System Administrator. It can track access and attempted access to the device and transmit audit logs to a SIEM system or audit log server. An example of an Audit Log entry: "User xx logged into the Xerox® AltaLink® MFP at 12:48 AM and faxed 10 pages to 888.123.1234."

For Xerox® ConnectKey® Technology-enabled multifunction printers, the Audit Log can be automatically and securely sent to a SIEM system to provide for continual monitoring of the MFP.



The Audit Log interface is accessed from a System Administrator's workstation using any standard Web browser.



The log can then be exported into a .txt file, and opened in Microsoft® Excel®.

Security Overview

4. External Partnerships

Xerox works with compliance testing organizations and security industry leaders such as McAfee to wrap their overarching standards and know-how around ours. The following malware protection features are available on Xerox® ConnectKey® Technology-enabled MFPs (Xerox® AltaLink® and i-Series Multifunction Printers).

MCAFEE® EMBEDDED CONTROL—ENHANCED SECURITY

Xerox® MFPs built on Xerox® ConnectKey® Technology include McAfee Embedded Control integration powered by Intel® Security, resulting in the industry's first lineup of multifunction printers that protect themselves from potential outside threats. McAfee's whitelisting technology detects unauthorized attempts to read, write or add to protected files and directories and sends alerts if they occur. Also, seamless integration with Xerox® CentreWare® Web Software, the Xerox® MPS toolset and McAfee ePolicy Orchestrator® (McAfee ePO™) allows for monitoring from the preferred console.

MCAFEE EMBEDDED CONTROL—INTEGRITY CONTROL

Integrity Control builds on the Enhanced Security capabilities and adds prevention of new files from being executed from any location by untrusted means. Only approved software is allowed to run, which prevents both general and targeted attacks. Useful especially for enterprise-wide security implementations, Xerox and Intel Security offer whitelisting technology that ensures the only function those devices are doing are the services you want to deliver. This same technology is used to protect servers, ATMs, point-of-sale terminals and embedded devices such as mobile devices.

MCAFEE'S EPOLICY ORCHESTRATOR (EPO)

McAfee's ePolicy Orchestrator (ePO) is a security management software tool that makes risk and compliance management easier for organizations of all sizes. It presents the users with drag-and-drop dashboards that provide security intelligence across endpoints—data, mobile and networks—for immediate insight and faster response times. ePolicy leverages existing IT infrastructures by connecting management of both McAfee and third-party security solutions to LDAP, IT operations and configuration management tools.

For third-party independent proof that we achieve top levels of compliance, certification bodies like Common Criteria (ISO/IEC 15408) and FIPS 140-2 measure our performance against international standards. They recognize us for our comprehensive approach to printer security.

CISCO® IDENTITY SERVICES ENGINE (ISE) INTEGRATION

Centrally manage and deploy printer security policies. Our partnership with Cisco provides greater Xerox® print device detection capabilities, resulting in finer-grain security policy enforcement. Xerox® devices are automatically recognized and classified by Cisco ISE, permitting network access control and reduction of overhead by eliminating manual entry of printer attributes. Our profiling of printers with Cisco ISE thwarts spoofing attempts by saboteurs to gain unfettered access to sensitive systems. Xerox® print device integration with Cisco ISE provides an operationally efficient approach to meeting security policy objectives.

Regulatory and Policy Compliance

Modern printers and MFPs are a focus for compliance due to the personal and sensitive data they access, store and communicate. Non-compliance can lead to lost business opportunities, losing existing customers or even legal action. Levels of required compliance vary by country and vertical market.

The Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the Data Protection Act in the UK are examples of standards that may need to be met to continue business legally.

Common Criteria Certification is an internationally recognized security standard that meets U.S. Department of Defense specifications.

With industry-leading security features and a flexible approach to configuration and deployment, Xerox® devices can conform to any standard and have the controls available to match any need.

Xerox® systems, software and services conform to recognized industry standards and the latest governmental security regulations. Our products offer features that enable our customers to meet those standards. The following standards are examples:

- Payment Card Industry (PCI) Data Security Standards Version 3.0
- Sarbanes-Oxley
- Basel II Framework
- The Health Insurance Portability and Accountability Act (HIPAA)
- E-Privacy Directive (2002/58/EC)
- Gramm-Leach-Bliley Act
- Family Educational Rights and Privacy Act
- The Health Information Technology for Economic and Clinical Health Act
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- ISO-15408 Common Criteria for Information Technology Security Evaluation
- ISO-27001 Information Security Management System Standards
- Control Objectives for Information and Related Technology
- Statement on Auditing Standards No. 70
- NIST 800-53, adopted by Federal Government and DOD in 2014
- Federal Risk and Authorization Program (FedRAMP)

Product Security Evaluation

Document security means peace of mind. One of the hallmarks of the Xerox® product line is a commitment to information security. Our systems, software and services comprehend and conform to recognized industry standards and the latest governmental security regulations.

Common Criteria Certification

Common Criteria Certification provides independent, objective third-party validation of the reliability, quality and trustworthiness of IT products. It is a standard that customers can rely on to help them make informed decisions about their IT purchases. Common Criteria sets specific information assurance goals including strict levels of integrity, confidentiality, availability for systems and data, accountability at the individual level and assurance that all goals are met. Common Criteria Certification is a requirement of hardware and software devices used by the federal government on national security systems.

Achieving Common Criteria Certification

Common Criteria Certification is a rigorous process that includes product testing by a third-party laboratory that has been accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluation of products against security requirements. Products are tested against security functional requirements based on predefined Evaluation Assurance Levels (EALs) or specialized assurance requirements.

For healthcare, financial services and other industries, the need for security is no less important. Whether they are protecting their customers' privacy, or intellectual and financial assets, assurance that networks, hard drives and phone lines are safe and secure from hackers, viruses and other malicious activities is critical. Common Criteria Certification, while not a requirement outside the federal government, can provide independent validation.

With approximately 150 devices having completed the certification process, Xerox has one of the largest numbers of Common Criteria Certified MFPs. In addition, Xerox was the first manufacturer to certify the entire device and Xerox is the only manufacturer to always certify the entire device.

Visit www.xerox.com/information-security/common-criteria-certified to see which Xerox® MFPs have achieved Common Criteria Certification.

Risk Assessment and Mitigation

Proactive Security for Emergent Threats

Offering you the market's most secure products and solutions today is just part of our story. Our scientists and engineers are hard at work developing the next generation of innovative security technologies to combat tomorrow's threats and keep your documents safe: micro-printing, fluorescence and infrared print security, Xerox® Glossmark® and Correlation Marks print mark technology, just to name a few. For more information about these technologies, visit www.xerox.com/security.

Other things Xerox does:

Keep a close eye on the latest risks

We closely monitor vulnerability clearinghouses to keep up to date on the latest information—so you don't have to.

Issue security bulletins

We're proactive in providing you with security patches and updates when necessary, keeping your equipment up to date and your data safe.

Distribute RSS feeds

Up-to-the-minute updates are automatically distributed to customers' RSS feed readers.

Provide you with a wealth of information

If you want to learn more on your own, we offer an ever-expanding library of security articles, white papers and guides.

Visit www.xerox.com/security to access our full breadth of security resources.

In addition to our own extensive internal testing, Xerox regularly monitors vulnerability clearinghouses made available by such entities and resources as US-CERT and Oracle® Critical Patch Updates report; Microsoft® Security Bulletins, for various software and operating system vulnerabilities; and bugtraq, SANS.org and secunia.com for open source vulnerabilities. A robust internal security testing program is also engaged that involves vulnerability analysis and penetration testing to provide fully tested patches. Visit www.xerox.com/security to read the Vulnerability Management and Disclosure Policy.

Security Bulletins and Patch Deployment

Xerox developers follow a formal security development life cycle that manages security problems through identification, analysis, prioritization, coding and testing. We strive to provide patches as expediently as possible based on the nature, origin and severity of the vulnerability. Depending on the severity of the vulnerability, the size of the patch and the product, the patch may be deployed separately or take the form of a new release of software for that product.

Depending on which Xerox® product requires a patch, customers can download security patches at www.xerox.com/security. For other Xerox® products, the security patch will be made available as part of a new release version of system software. You can register to receive bulletins regularly. In the U.S., customers should sign up for the security RSS feed. Outside the U.S., contact your local Xerox support center.

From the www.xerox.com/security website, you have access to timely information updates and important resources:

- Security Bulletins
- RSS Feed: Get Security Bulletins
- Xerox® Product Security Frequently Asked Questions
- Information Assurance Disclosure Papers
- Common Criteria Certified Products
- Vulnerability Management and Disclosure Policy
- Product Security Guidance
- Articles and White Papers
- Statements of Volatility
- Software Release Quick Lookup Table
- FTC Guide for Digital Copiers and MFPs



www.xerox.com/security is your portal to a diverse breadth of security-related information and updates, including bulletins, white papers, patches and much more.

Manufacturing and Supplier Security Practices

Xerox and our major manufacturing partners are members of the Electronic Industry Citizenship Coalition (<http://www.eicc.info>). By subscribing to the EICC Code of Conduct, Xerox and other companies demonstrate that they maintain stringent oversight of their manufacturing processes.

Also, Xerox has contractual relationships with its primary and secondary suppliers that allow Xerox to conduct on-site audits to ensure the integrity of the process down to the component level.

Xerox also is a member of the U.S. Customs Agency Trade Partnership Against Terrorism. This initiative is focused on supply chain security. Examples of practices adopted by Xerox under this program are those put in place to counter theft or hijacking. Within North America, all trailers moving between the factory and the product distribution centers (PDCs), and between the PDCs and Carrier Logistics Centers (CLCs) are sealed at the point of origin. All trucks have GPS locators installed and are continuously monitored.

Product Returns and Disposals

Hard Drive Retention Offering for Xerox® Products

Xerox provides a Hard Drive Retention Offering to allow customers in the United States, for a fee, to retain the hard drive on leased Xerox® products. This service may be required for customers with very sensitive data, perhaps classified, or with internal policies or regulatory standards that mandate specific disposition processes for hard drives.

Upon request for this service offering, a Xerox service technician will travel to the customer location, remove the hard drive and provide it 'as is' to a customer representative. At this time, Xerox does not provide hard drive sanitization, cleansing or destruction services on site at customer locations. Customers will need to make arrangements for final disposition of the physical hard drive received from the technician.

To determine if your Xerox® product contains a hard drive or review security features available to secure data on hard drives, please visit www.xerox.com/harddrive.

For more details about this program, contact your Xerox sales representative or visit www.xerox.com/security under Security Resources in the Articles and White Papers section.

Additionally, virtually all new Xerox® printers and MFPs come standard with 256-bit AES disk encryption, as well as 3-pass image data overwrite to ensure our customers' data is protected from day one on their new equipment.

Summary

Network and data security are among the many challenges that businesses face on a daily basis. And because today's printers and MFPs serve as business-critical network devices that receive and send important data through a variety of functions, ensuring comprehensive security is paramount.

An MFP's entire system, along with any device management software on the network, must be evaluated and certified so that Information Security and all the workers of an organization are certain that their documents and network are safe and secure from information predators—or even from internal security breaches. In that respect, Xerox® MFPs lead the industry. Our comprehensive approach, based on foundational, functional, advanced and usable security, is critical to safeguarding our customers' information assets.

Recognizing this, Xerox continues to engineer and design all of its products to ensure the highest possible level of security at all potential points of vulnerability. We're committed to safeguarding your data so you can focus on the pursuits and activities that make your business or organization as successful as possible.

For more information about the many security advantages offered by Xerox, visit www.xerox.com/security.

Security Checklist

IT security managers are already overwhelmed with managing security demands. Small businesses must rely on effective systems and security software to do much of the work for them. The last thing you and your staff need is more high-touch activity or manual interventions to monitor and keep updated every device and data stream in your environment, including your MFPs and printers.

A comprehensive network security plan should include three points of emphasis, with a strategy in place for each to ensure you have a plan that works.

1. “Hands-off, self-protecting” devices that are resilient to new attacks
2. Compliance with the most up-to-date security standards and regulations
3. Complete visibility on the network

The New Security Standard for a New Age

- Security cannot be an afterthought.
- Information is an increasingly valuable intellectual property.
- Firewalls aren’t enough; security policies must be holistic and ubiquitous.
- Protection for embedded devices is now an integral part of today’s security imperative.

Xerox offers comprehensive, multi-layer security that is easy to deploy and manage, and helps keep your business compliant with industry and government standards. Xerox® technology is tested and validated to protect against unauthorized access, data and identity.

When comparing Xerox® MFPs with other manufacturers’ products, use the following checklist to determine whether the competitors’ devices provide the same level of end-to-end security as delivered by Xerox.

	Xerox	Competitor		
		1	2	3
IP/MAC Address Filtering	✓			
IPsec Encryption	✓			
IPv6	✓			
802.1X Authentication	✓			
Secure Print	✓			
Scan to Email Encryption	✓			
Encrypted PDF/Password-Protected PDF	✓			
Digital Signatures	✓			
256-bit AES Hard Disk Encryption	✓			
Image Overwrite	✓			
Secure Fax	✓			
Port Blocking	✓			
Scan to Mailbox Password Protection	✓			
Hard Drive Retention Offering	✓			
Print Restrictions	✓			
Audit Log	✓			
Role Based Access Control	✓			
Smart Card Authentication	✓			
Common Access Card/Personal Identity Verification	✓			
User Permissions	✓			
“Full System” Common Criteria Certification	✓			
Integration with Standard Network Management Tools	✓			
Security Updates Via RSS Feeds	✓			
Embedded McAfee Protection Powered by Intel® Security	✓			
McAfee® Integrity Control	✓			
McAfee® ePolicy Orchestrator® Integration	✓			
Cisco® Identity Services Engine (ISE) Integration	✓			

To learn more, visit www.xerox.com.

©2018 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design®, AltaLink®, CentreWare®, ConnectKey®, Global Print Driver®, GlossMark® and VersaLink® are trademarks of Xerox Corporation in the United States and/or other countries. 4/18 BR21699 SECGD-01UH





Xerox[®] Device Manager Certification Guide

Xerox Confidential

©2018 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design®, Xerox Nuvera®, Phaser®, VersaLink®, AltaLink®, iGen®, WorkCentre®, CentreWare Web, and Xerox® ConnectKey® Technology are trademarks of Xerox Corporation in the United States and/or other countries. BR22537

Microsoft®, Windows®, SQL Server®, and Internet Explorer® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Novell® and Netware® are trademarks of Novell, Inc. in the United States and other countries.

To ensure the efficient fulfillment of Xerox service offerings, we leverage global competency centers and cloud technology. This may result in the personal data we process being transferred beyond the European Economic Area (EEA), but within the parameters of the defined service offering. The level of protection afforded by General Data Protection Regulation (GDPR) is not undermined through data transfers, and all transfers undertaken by Xerox are carried out in full compliance with GDPR using an approved mechanism and subject to appropriate safeguards.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Revision History

Version	Date	Description
6.3	October 2018	Addressed remote SQL database workload behavior, Fleet Orchestrator to firm-ware upgrade options, new CWW Customer Report User role,permissions requirements for Certificate Management
6.2	May 2018	Added note about personal data processing for GDPR, removed support for SQL Server 2008
6.1	October 2017	Rebranded. Updated supported versions of SQL Server and Windows Server.
6.0	May 2017	updated supported browsers, hardware and SQL requirements, firmware upgrade details
5.15	February 2016	Added support for SQL 2014 and Microsoft Edge. New section for Setting Additional SNMP V3 Encryption and authentication
5.14	October 2015	Added recommendation example to Hardware and Software Requirements Updated the Windows Server Security Section with FIPS note and admin rights note
5.13	June 2015	Added Windows Event Viewer, updated the Printer Fields Exported to Xerox® Services Manager table, and update version of .NET

Table of Contents

How to Use This Guide	2
Intended Audience	2
FAQ Related to Implementation	2
Using This Guide	2
Limits to This Guide	3
Certification Roles and Responsibilities	3
Customer IT Organization	3
Enterprise Print Services – Office Organization	3
Ongoing Operational Roles and Responsibilities – Xerox® Device Manager Site Maintenance	3
Product Overview	6
Requirements	7
Xerox® Device Manager Communication with Devices	7
Hardware and Software Requirements	7
SQL Server Licensing Requirements	9
Remote SQL Database Workload Behavior	9
Software Requirements	9
Network Printer Requirements	10
Client Software Requirements	11
Browser Requirements	11
Browser Settings	11
Additional Recommendations for Client Browsing to MPS	12
SNMP Services	12
SNMP V3 Security Enhancements	12
Services Used by the Xerox® Device Manager Application	13
Check the Windows Firewall Status	13
Security	15
Windows Server® Security	15
SQL Server Security	15
Internet Information Services (IIS) Security	15

Xerox® Device Manager Configuration Sets Feature	16
SNMP Security	16
SNMP v1-v2 Security	17
SNMP v3 Security Enhancements	17
Users and Groups	17
CWW-Specific Groups	17
The Run As Account	18
Required Permissions	19
Windows Considerations	20
Printer Information Communicated to Xerox® Services Manager	20
Xerox® Device Manager Server Information Exported to Xerox® Services Manager	21
Xerox® Device Manager Job Accounting Data Exported to Xerox® Services Manager	21
Xerox® Device Manager Policy Log Data Exported to Xerox® Services Manager	24
New entry	24
Corporate Security Mode	24
Remote Commands from Xerox® Services Manager	25
Remote Configuration	25
Additional Administration Capabilities	26
Xerox® Device Manager Logs	28
Action Log	28
Audit Log	28
E-mail Log	28
Event Log	28
Systems Infrastructure	30
Network Ports Used by Xerox® Device Manager	30
Windows® Services Utilized by Xerox® Device Manager	31
General Discovery Considerations	31
Discovery Network Data Calculations	34
Network Impact Considerations of Status Polling	35
Scheduled Communications Calculations	35
SNMP Alerts Traffic Calculation	35
Active Directory® Customer Import Network Data Calculations	36
Total Xerox® Device Manager Data Transfer Calculations	36
Email Data Comparison	37

Production Device Job Data Transfer	38
Integrations with Xerox® Services Manager and the Hosted Deployment Model	40
Xerox® Device Manager to Xerox® Services Manager Interactions	40
Alternative Device Discover Methods	43
IP Easy Discovery	43
Operation	43
When to Use	43
Network Impact	43
Accuracy	43
IP Broadcast	43
Operation	43
When to Use	44
Network Impact	44
Accuracy	44
IP ARP Cache Discovery	44
Operation	44
When to Use	46
Network Impact	46
Accuracy	46
IP Sweep	46
Operation	46
When to Use	46
Network Impact	46
Accuracy	47
SNMP V3 IP Sweep	47
Operation	47
When to Use	47
Network Impact	47
Accuracy	47
Subnet Scan	47
Operation	47
When to Use	48
Network Impact	48
Accuracy	48

IPX Network Scan Discovery	49
Operation	49
When to Use	49
Network Impact	49
Accuracy	50
IPX Server Discovery	50
Operation	50
When to Use	51
Network Impact	51
Accuracy	51
IPX Address Scan Discovery	51
Operation	51
When to Use	52
Network Impact	52
Accuracy	52
Summary and Next Steps	54
Appendix	55
Firmware Upgrade Information	55

How to Use This Guide

This guide is designed to help customer organizations certify the deployment of Xerox® Device Manager, a front-end software component of the Xerox Managed Print Services (MPS software suite). The document contains information related to Xerox® Device Manager's potential impact to security, enterprise IT infrastructure, network traffic, resources, and required planning.

The certification guide is meant to be used primarily during implementation and after contract signature, but it can also be used during pre-sales and evaluation activities.

Because the Xerox® Device Manager software typically is installed within the customer's network environment, this guide also covers key aspects of the back-end MPS software components. Xerox support teams operate the back-end applications from the secure remote MPS hosted facility, as facilitated by MPS/Xerox® Device Manager interoperability.

Intended Audience

This guide will be used by the customer's IT, security, and management organizations as well as by Xerox management. Before certifying Xerox® Device Manager, customers and appropriate Xerox personnel should have a clear understanding of:

- the IT environment at the site where Xerox® Device Manager will be installed,
- the IP topography (addresses, subnets, and gateways),
- any restrictions placed on applications that are deployed on that network, and
- the Microsoft® Windows Server® operating system.

FAQ Related to Implementation

These are some of the questions that this certification guide should address for the IT staff:

- What additional hardware and software will be introduced to my IT environment?
- What typical loads and bandwidth demands will be made on my network?
- What new user accounts will be created and what existing accounts (if any) will be touched by this application?
- What network protocols and IP ports will be used by this application?
- What levels of security are incorporated within/around Xerox® Device Manager?
- What will the impact to my printing environment be after this application is installed?
- What other impacts/effects to people, processes, or products will occur?
- What considerations should be given to those who perform the periodic backup of the Xerox® Device Manager Microsoft® SQL Server® database, and if applicable, the database restore?

Using This Guide

This guide is meant for customer and Xerox personnel to use as part of the evaluation, testing, and acceptance process. Actual test plans and acceptance criteria are dependent upon the formality or

required documentation of the customer. Responsible areas include security, network, IT Infrastructure, test organization if required, and output device operations personnel.

Limits to This Guide

This guide is intended to be the initial information source for MPS customer IT organizations—specifically, a review of those Xerox® Device Manager features that may have a discernible impact to the customer IT environment. The Xerox® Device Manager software is highly configurable and has many features. This guide is based on a standard implementation and a typical customer IT and printer environment.

If the customer's IT environment differs from what is described in this guide, then the customer's IT team and the Xerox Managed Print Services representative need to identify the differences and resolve any potential concerns.

The guide's information is related to the Xerox® Device Manager 6.3.x release. Although much of this information will remain constant through the software's life cycle, some of the data provided may be revision-specific, and will be revised periodically. IT organizations should check with the Xerox representative to obtain the appropriate version.

Certification Roles and Responsibilities

CUSTOMER IT ORGANIZATION

Ultimately, it is the responsibility of the customer's IT organization to certify and accept the deployment and operation of the Xerox® Device Manager software and server within their network environment. The customer may have an informal certification process, which is limited to the review of MPS documentation and a Xerox demonstration. Or, the customer may have a more formal process that requires actual installation and testing with defined test criteria and test plan. The customer needs to define the certification criteria, and work with the Xerox team to define the required steps and timeline.

ENTERPRISE PRINT SERVICES – OFFICE ORGANIZATION

Xerox personnel will participate in the certification process, and determine which Xerox® Device Manager features and functions are required and the frequency of Xerox® Device Manager activities.

Ongoing Operational Roles and Responsibilities – Xerox® Device Manager Site Maintenance

As part of the customer certification process, the Xerox account team, also known as the Operations Team, and the customer's IT organization need to define the roles and responsibilities for the ongoing care of the Xerox® Device Manager software installation:

- Who will be responsible and what is the planned schedule for periodic backups for the SQL database that Xerox® Device Manager uses in its operation? If the account is “unstaffed” with Xerox personnel, then the IT organization needs to include the Xerox® Device Manager database within their periodic database backup schedule, which they may perform on other systems. In the case that instructions for performing MS SQL Server database backups and restores are needed, the instructions for these operations can be found in the Xerox® Device Manager Read Me file, which is part of the Xerox® Device Manager software installation (Program Files\Xerox\Xerox Device Manager\Readme.txt).

- If an installation includes server hardware, what will be the standard practice for performing the periodic Microsoft® operating system software update? Typically, the Xerox® Device Manager server will have to follow the software update policies of the customer's IT organization, but the two parties need to discuss and agree to this standard practice.
- If Xerox staff will not be managing Xerox® Device Manager for a customer's account, who will be responsible for installing required patch upgrades to Xerox® Device Manager?

Product Overview

Xerox® Device Manager is the front-end application of the Managed Print Services (MPS) suite that discovers, installs, configures, manages, monitors, and reports on any type of SNMP-based printing device attached to an IP network, regardless of manufacturer. Xerox® Device Manager communicates all of this information via a secure link to the Xerox MPS hosted facility. Xerox® Device Manager is Xerox proprietary software and part of the infrastructure that facilitates the delivery of managed print services by Xerox personnel, which only Xerox personnel can access.

Xerox® Device Manager discovers network-connected printers within designated areas of an enterprise (via IP subnets). Xerox® Device Manager conducts status and meter polling as well as collects device and status history information. Xerox® Device Manager provides clear and concise status for all networked printers, with the ability to group printers as required for reporting. In summary, Xerox® Device Manager performs the following:

- gathers and reports on printer status
- discovers and manages network-connected printers and print servers
- collects meter and device history information
- monitors printers and print servers for status and alert conditions with auto ticket creation
- initiates troubleshooting tests on single printers (or multiples in a group) and display the results
- creates and manages configuration sets used to setup printers and multi-function devices
- upgrades printer firmware
- installs and manages local and remote print queues
- communicates required information to the secure hosted site

Xerox® Device Manager can also discover Locally Connected (Direct) printers attached to computers providing basic printer information, and in some cases, detailed information that includes Meters and Consumable Levels. Detailed information is dependent on what the Direct Printer supports.

All contract reporting will come from the hosted facility application, Xerox® Report Manager. Xerox® Device Manager also has limited reporting capability, which may be used for archive or validation purposes, such as reports on device alert history tables and a security audit report.

Requirements

Xerox® Device Manager Communication with Devices

Xerox® Device Manager supports both industry-standard and private SNMP MIBs; however, the amount and types of management that Xerox® Device Manager can provide is dependent on the printer's level of conformance to these coding standards, such as:

- Device Identity (e.g., model, serial number, manufacturer, etc.)
- Device Properties (e.g., input trays, output bins, serial number, etc.)
- Device Status including overall state, detailed status, UI messages, etc.
- Consumables + levels (toner, fuser, print cartridge, + device unique parts)
- Supported PDL interpreters (PostScript, PCL, TIFF, PDF, automatic, etc.)
- Supported print protocols (LPD, HTTP, Port 9100, Netware PServer, etc.)
- TCP/IP protocol suite (SNMP, TCP, UDP, IP, NIC details, etc.)
- Finishing options (hole punch, fold, staple, stack, booklet, etc.)
- SNMP v3-based trap registration

Xerox® Device Manager also collects information from private MIBs for most manufacturers where the device is not coded to the industry standard. The collected information may include the following:

- Device firmware and possible upgrade
- Device configuration cloning
- Detailed usage counters
- SNMP based trap registration
- Detailed network protocol configuration settings
- Network scanning configuration settings on multi-function devices (MFDs)

Xerox® Device Manager can also obtain basic information from Direct printers attached to Computers. There are two ways that Xerox® Device Manager can discover the Direct printers:

1. Discovery of Computers and their Direct printers: Computer Discovery uses by default ICMP and NetBios File and Print sharing protocols for Computer/Direct Printer discovery, but can be expanded to use WMI over RPC when ICMP is not supported. This method provides basic information about the printers, and does not include meter information or consumable levels. See the Required Permissions section for information on what user permissions are needed to discover Computers and their Direct Printers.
2. Xerox® Printer Agent: Xerox® Printer Agent clients installed on computers that have Direct Printers can report to an Xerox® Device Manager server about the direct printers attached. Basic printer information is provided with additional detailed information (meters, consumable levels, etc.) for printers that support querying of the detailed information.

Note: Refer to the Xerox® Print Agent Certification Guide for more details on Xerox® Print Agent and the specific data gathered by a Xerox® Print Agent client.

Hardware and Software Requirements

These are the minimal hardware requirements. Depending on the number of devices being managed and the configuration of the Xerox® Device Manager server, you may need a more advanced hardware configuration or multiple servers.

Hardware Requirement	Recommendations
Processor	Intel® Pentium® 4 processor at 3 GHz or Intel® Core 2 duo (AMD equivalent processors are supported as well)
Memory	4 GB of RAM, with one of the following versions of SQL® Server installed on the same system: <ul style="list-style-type: none"> • 2012 • 2014 (Recommended) • 2016 (Recommended) • 2017 (Recommended) • SQL Express®
Server	A separate server with SQL installed is highly recommended if: <ul style="list-style-type: none"> • the number of groups configured for concurrent status polling is greater than 20 and/or • the number of alert profiles is greater than 20 and/or • Job data consumption is greater than 100,000/week.
Available Disk Space	Minimum: 3GB Recommended: 40GB on 7200 rpm hard drive if collecting historical data on thousands of devices.

Table 1: Hardware Requirements

Recommended Hardware Operating System And SQL Requirements:

For Installs < 5000 Devices:

- Xerox® Device Manager on Windows Server 2008R2 with off-box SQL*
 - 2 CPU cores @2.9 GHz
 - 4 GB RAM
 - 40 GB free space (preferably on a non-system disk)
- Xerox® Device Manager on Windows Server 2008R2 with on-box SQL/SQL Express**
 - 2 CPU cores @2.9 GHz
 - 8 GB RAM
 - 60 GB free space (preferably on a non-system disk)
- Xerox® Device Manager on Windows Server 2012R2 with off-box SQL*
 - 2 CPU cores @2.9 GHz
 - 12 GB RAM
 - 40 GB free space (preferably on a non-system disk)
- Xerox® Device Manager on Windows Server 2012R2 with on-box SQL/SQL Express**
 - 2 CPU cores @2.9 GHz
 - 16 GB RAM
 - 60 GB free space (preferably on a non-system disk)

* Use the newest version of SQL acceptable to the customer.

** On-box SQL is only recommend for very small installations (< 200 devices)

For Installs > 5000 devices:

- Use an off-box SQL Server
- Increase memory by 50%

- Add 2 CPU cores

For Installs > 10,000 devices:

- One terabyte disk space
- 6 GB RAM
- Quad Core 3.4 Ghtz processor
- SQL Enterprise on separate server

If running on a virtual system, all resources need to be dedicated to Xerox® Device Manager.

Note: In the event that you need to install Xerox® Device Manager on a rack-mounted server, it is expected that a Keyboard-Video-Mouse terminal interface to the server will be provided.

SQL SERVER LICENSING REQUIREMENTS

When deploying Xerox® Device Manager, you have to consider the SQL Server® licensing because Microsoft offers a number of licensing options. If you are going to use an Express version, be aware that since it uses a single processor license, you do not have to consider the number of connections. If you are going to an Enterprise version, you need to consider the licensing option. If you are going to use CAL licensing, Xerox® Device Manager requires a minimum of three CALs, which covers only the application and local access to the server. If you have any connections to help you manage Xerox® Device Manager through a browser or if you have any print server/workstation that is running the Xerox® Print Agent, you will need an additional CAL for each one.

Note: You have the ability to change the SQL Server database names during installation. When multiple Xerox® Device Manager servers are required and you must use a remote SQL Server, you can install the different Xerox® Device Manager servers on the same instance of the SQL Server by giving the Xerox® Device Manager SQL Server databases different names.

REMOTE SQL DATABASE WORKLOAD BEHAVIOR

In most cases the database workload behavior of Xerox® Device Manager is OLAP. However, please note that for configuration setting updates that involve large fleets the system can exhibit behavior consistent with Batch or ETL workloads. Customer choices for management of features (updates vs audit) and scheduling of configuration policies (immediate vs off hours) will affect the workload behavior.

SOFTWARE REQUIREMENTS

Software Requirements	Supported
Operating Systems	Windows® 2008 R2 x86 and x64 Windows® 2012 and 2012 R2 Windows® Server 2016 x64 Note: Xerox® Device Manager does not support Windows® systems running on a Novell® client, Macintosh®, or non-NTFS partitions. Note: Xerox® Device Manager does not support installation on a Domain Controller.
Web Server	Internet Information Services (IIS) 6.0 or above
Internet Protocol	Working Microsoft® TCP/IPv4 Stack
Browser	Internet Explorer® 9.0, 10, 11 Microsoft Edge
Access Components	Windows Data Access Components (WDAC): MDAC changed its name to WDAC (Windows Data Access Components) and Windows Server 2008. WDAC is included as part of the operating system and is not available separately for redistribution. Ser-

Software Requirements	Supported
	viceability for WDAC is subject to the life cycle of the operating system.
Microsoft® .NET Framework	Microsoft® .NET 4.5.2 Note: The .Net Framework is not installed with Xerox® Device Manager and needs to be installed prior to running the installation for Xerox® Device Manager.
Microsoft® Core XML Services	6.0 required for some of the application's functionality
Database Server	Recommended: Use SQL Server® Standard/Enterprise if available in the customer's IT environment. Note: If using a remote SQL Server, both the remote client on which SQL Server is installed and the Xerox® Device Manager Server client require the Microsoft® Distributed Transaction Coordinator (MSDTC) service to be enabled and configured in order to allow remote client access. If the Windows® Firewall is running a firewall, an exception needs to be created for the MSDTC service. Note: When managing more than 5,000 devices or using the Xerox® Print Agent feature, we recommend that you install a SQL Standard/Enterprise version of SQL on a separate server. The requirements for the separate database server should match the requirements for the Xerox® Device Manager server. Note: If using an Azure SQL Services installation, the following components need to be installed and the server rebooted prior to installing Xerox® Device Manager 6.3: 1. Windows Management Framework 5.1 (Windows Server 2016, 2012 R2 or 2012*) *not available for Server 2008 or Server 2008 R2. 2. Azure Powershell 6.7.0 or later can be downloaded here from https://github.com/Azure/azure-powershell/ Both *x86 or x64 (default) should work.

Table 2: Software Requirements

Network Printer Requirements

For a full Xerox Office Services implementation, Xerox® Device Manager will require access to the Internet via SSL for integration with Xerox® Services Manager. For successful management by Xerox® Device Manager, all SNMP-based printer devices should support the mandatory MIB elements and groups as defined by the following standards:

Network Printer Discovery/Monitoring Requirements	Recommendations
RFC 1157	SNMP Version 1
RFC 1213	MIB II-for TCP/IP-based Internet
RFC 1514/2790	Host Resources MIB v1/v2
RFC 1759	Printer MIB v1
RFC 3805	Printer MIB v2
RFC 3806	Printer Finishing MIB
Optional: RFC 2271-2275	SNMP V3 Architecture

Table 1: Hardware Requirements

Client Software Requirements

The following sections discuss the requirements for PC access to the Xerox® Device Manager Web-served application.

BROWSER REQUIREMENTS

Although the Xerox® Device Manager server can be used to directly browse to the Xerox® Device Manager application, in some cases, it is necessary for Xerox Managed Print Services personnel to access the application from a desktop. The supported browsers for Xerox® Device Manager are Internet Explorer 9.0, 10.0, 11.0 and Microsoft Edge.

Note:

- Transmission Control Protocol/Internet Protocol (TCP/IP) must be loaded and operational.
- To use the IPX Network features of Xerox® Device Manager, an IPX protocol stack must be loaded and operational on the Xerox® Device Manager server.
- In environments supporting devices with IPv6 addresses, Internet Explorer 9.0 or above should be installed to enable printer images to be visible on the Device Details page in Xerox® Device Manager.

BROWSER SETTINGS

The following settings should be applied to any browser connecting to the MPS software.

1. From **Tools>Internet Options>Advanced**, locate the HTTP 1.1 settings node in the settings. Use HTTP 1.1 is required, and should already be checked. Use HTTP 1.1 through Proxy connections is required if you are behind a proxy server. Check with your local Desktop Administrator if you are unsure. Scroll further in the Advanced tab options, to the Security section. For application Security, uncheck Do not save encrypted pages to disk. For application performance: check Do not save encrypted pages to disk.
Note: For Security, uncheck Do not save encrypted pages to disk. Application performance will be heavily degraded. Verify this setting with your local Desktop Administrator first.
2. Check **Use SSL 3.0** and **Use TLS 1.0, TLS 1.1, and TLS 1.2**. (Verify this setting with your local Desktop Administrator first).
Note: We recommend that you use the most recent and, therefore, most secure version when possible. Some Microsoft security patches have disabled TLS 1.0 and 1.2 on targeted systems. An Administrator needs to manually re-enable 1.0 and 1.2, if those versions are desired. Additionally, some older devices may not support TLS 1.2 without the latest system firmware. As a result, you may experience incompatibility with your system and select devices. A hybrid approach is necessary in such cases.
3. Check Warn if forms submission is being redirected. (Verify this setting with your local Desktop Administrator first.)

The remaining settings on this tab have no bearing on MPS security or performance:

1. From **Tools>Internet Options>Privacy: Advanced**
2. There are two acceptable settings for this option. This is a required setting, but either of the two choices is acceptable. The first is for the Override automatic cookie handling box to be unchecked. This is the default setting. If the Override automatic cookie handling box is checked, under First-party Cookies the radio button for Accept should be selected. Always allow session cookies should also be selected. The Third-party Cookies option has no bearing for the MPS applications. Verify with your local Desktop Administrator which cookie handling setting is appropriate for your site.
3. From **Tools>Internet Options>Privacy: Settings**, if the Block pop-ups option is checked, click the Settings button to edit these settings. Add *.services.xerox.com to the list of Allowed Sites. This setting change

- also applies to any third-party popup-blockers. (Verify this setting with your local Desktop Administrator first).
4. From **Tools>Internet Options>General>Temporary internet file settings**, make sure that Check for newer versions of stored pages is set to Automatically. Make sure that the Amount of disk space to use: is set to at least 500 Mb.
 5. From **Tools>Internet Options>Security**, click the Trusted sites Web content zone, and click the Sites button. Add <https://office.services.xerox.com> and <https://reporting.services.xerox.com> to the list of Web sites. Make sure that Require server verification (https:) for all sites in this zone is selected.

ADDITIONAL RECOMMENDATIONS FOR CLIENT BROWSING TO MPS

1. If your Anti-Virus product has a script scanning feature, this feature should be disabled or *.services.xerox.com should be added to the list of excluded sites. (**Optional:** However, application performance could be heavily degraded if script scanning is enabled. Verify this setting with your local Desktop Administrator.)
2. If you are running third party pop-up blockers, you should add *.services.xerox.com to the list of allowed sites.

SNMP Services

The Windows® “SNMP Service” installs an SNMP agent on the server and can respond to SNMP-based requests for information.

- WIN SNMP APIs are not used. Instead of using WinSNMP API to decode and encode packets Xerox® Device Manager uses the Xerox SNMP encoding/decoding mechanism. The Xerox® Device Manager SNMP communication infrastructure is completely .NET managed and .NET runtime provides fundamental security benefits which include, but are not limited to, invalid pointer manipulations, buffer overruns and bounds checking.
- Unless there is a local requirement to utilize the Microsoft® SNMP service, it should be disabled on the Xerox® Device Manager server. The Xerox® Device Manager server is only at risk if the Windows® “SNMP Service” is installed and running.
- The Windows® SNMP Trap service should also be disabled in order for Xerox® Device Manager to receive SNMP traps.

Note: The SNMP agent service, which ships with Windows® platforms, is not installed or running by default.

- The SNMP protocol can be disabled on several newer network printers as well. If this protocol is disabled, the Xerox® Device Manager application will not be able to discover these newer printers.
- The SNMP protocol may be blocked at the router level on one or more of the customer’s subnets. If this is the case, the Xerox® Device Manager application will not be able to discover printers connected to these subnets.

SNMP V3 SECURITY ENHANCEMENTS

SNMP is the most widely used in-band management protocol used for communication among network management stations and the devices being managed. In its current form, SNMP’s security is limited to three methods of access: Read-only, Write-only and Read-write. Access from the management station (Xerox® Device Manager) to the devices is granted by “community strings,” which are simply the groups to which the devices belong. Although disabling the write function in SNMP can prevent most in-band attacks, SNMP is a relatively insecure protocol, with nothing more than the community strings acting as passwords.

The SNMP V3 framework supports multiple security models, which can exist simultaneously, within an SNMP entity. SNMP V3 messages contain a field in the header that identifies which security model must process the message. To ensure some form of interoperability, a User-based Security Model (USM) is implemented to defend against unauthorized modification of managed elements and spoofing. Although SNMP V3 is a huge step forward in secure manageability, it cannot prevent "denial-of-service" attacks. In addition, its security system must stand alone, meaning every device must have a database of users/passwords. Since this is not likely to happen in most companies, all devices are left at risk.

Note: Refer to the Enabling High Security Guide for further SNMP v3 information and deployment considerations.

Services Used by the Xerox® Device Manager Application

The following services are used by the Xerox® Device Manager application:

- Remote Procedure Call
- Windows® Management Instrumentation(Used for detailed computer information during IP Domain Discovery or Managed Printer Server operations)
- MSSQL\$XEROXCWW (if selected default SQL option during install, otherwise the SQL Server® service selected during install)

The following services are a part of the Xerox® Services Manager applications:

- Xerox® Discovery Service
- Xerox® Schedule Service

A list of the services in use is available from the Xerox® Services Manager interface to registered Device Managers.

CHECK THE WINDOWS FIREWALL STATUS

Certain Windows Firewall settings are required to allow the server to be added as a managed print server, which allows the Xerox® Device Manager server to communicate with the Xerox Print Agent on peer computers and to get basic properties from any computer discovery. To retrieve additional detailed computer properties, Windows Firewall must be disabled.

To check the configuration of the Windows Firewall software perform the following:

Windows Server® :

1. Select **Start> Control Panel> Windows Firewall.**
2. Select **Change Settings.**
3. Select Exceptions tab. Enable the File and Printer Sharing program and select **OK.**
4. Select **Start> Administrative Tools> Windows Firewall with Advanced Security.**
5. Select **Inbound Rules.**

Make sure the File and Printer Sharing (Echo Requests) are enabled. The correct enablement should happen when the File and Printer Sharing Exception has been enabled.

Security

Security is an important consideration when evaluating tools of this class. This section is intended to provide some background into the security methods used by Xerox® Device Manager and offer some information on changing security-related defaults, if required.

Windows Server® Security

Xerox® Device Manager uses the security features built into Microsoft Windows Server® operating system including:

- User authentication and authorization
 - The User requires a Domain/Local service account with full administrator rights
- Services configuration and management
- Group policy deployment and management
- Internet Connection Firewall (ICF) including:
 - Security Logging settings
 - ICMP settings
- FIPS 140-2 compliant

SQL Server Security

Xerox® Device Manager uses the security features of both SQL Server Express and SQL Server including SQL Server user account registration and DSN encryption. During Xerox® Device Manager installation, a non-standard SQL Server network port can be used if desired. This port cannot be changed after installation. During Xerox® Device Manager installation, the user will need SQL Server administrative rights, while Xerox® Device Manager will only need DBO rights after installation. During Xerox® Device Manager installation, the account used to install Xerox® Device Manager requires the SQL Server administrative rights (i.e., sys_admin). After installation this role may be revoked, and the Xerox® Device Manager account will only need DBO rights after installation. As with many applications, customers must take extra care to prevent unauthorized use and abuse. Therefore, it is important to keep all servers and applications updated with the latest patches and service packs.

Internet Information Services (IIS) Security

IIS, as a Web page server, is an area that requires particular attention in terms of security. The following are security-related recommendations for using IIS with Xerox® Device Manager.

- Apply the latest Service Packs and Critical Updates available from Microsoft.
- Leave basic authentication off – With basic authentication on, the username and password are clear text-based and pose a potential security issue. When it is turned off, client browsers must connect to these secure areas via Windows® authentication.

If more security measures need to be employed at this site, first consider using native IIS security features such as:

- Use alternative Web site other than the default – Xerox® Device Manager can be configured to use a different Web site other than the default Web site set during installation.
- Change the HTTP port number – In IIS, the port number used for the Xerox® Device Manager server can be modified on the default Web site, which is part of the installation, or on another Web site that you have configured Xerox® Device Manager to use.
- Restrict access to the Web site to specific IP addresses – Modify the access via the properties on the Default Web site found in the IIS snap-in.
- Consider turning off anonymous authentication to all of Xerox® Device Manager – By default, no password is required to access the view-only Xerox® Device Manager pages.
- Use secure communications such as HTTPS/SSL/certificates.

Xerox® Device Manager Configuration Sets Feature

Within any managed site, there may be a need to manage the settings common to various machines efficiently and effectively. Xerox® Device Manager's Configuration Sets functionality can provide this capability to significantly aid in conformance stability. Configuration Sets are extremely useful with a large fleet of devices and/or where there is a high level of device moves, adds, or changes because they provide a reusable template to both monitor and set device configuration parameters. Configuration Sets are currently compatible with a variety of the Xerox® networked models. Configuration Sets have the ability to:

- expose and display open TCP and UDP ports on any network printer to identify potential security holes within the print environment
- lock the device console to prevent tampering
- inspect printer protocols and service settings for unauthorized changes
- turn on authentication for network scanning
- disable unused protocols and services on Xerox® network printers
- define SNMP Get/Set/Trap community names
- manually add SNMP v3-compliant printers in order to authenticate and encrypt all communication between them
- set the Image Overwrite capability
- set the Feature Installation Key across a fleet of eligible devices
- enable weblet for remote installation on Xerox® ConnectKey® Technology devices
- enable remote access to the console panel on ConnectKey devices

SNMP Security

The Simple Network Management Protocol (SNMP) is the most widely-used-network-management tool for communication between network management stations and the managed devices. Xerox® Device Manager uses SNMP during its discovery operations to provide detailed information about printers it finds on the network. After discovery, SNMP monitors printers for faults and changes in status, to carry configuration set changes and support printer troubleshooting.

SNMP V3 is the latest version on SNMP and, as such, is the most secure and supported. We recommend that you use SNMP V3 whenever possible, including in conjunction with V1 and V2. In some instances, OS support will not be available for SNMP V3. In such cases, use V1 and V2.

SNMP V1-V2 SECURITY

In SNMP v1/v2, security is limited to three methods of access: Read-Only, Write-Only, and Read-Write. **Community strings**, which are the names of the groups that the devices belong to, provide access from the management station to the devices. You can configure Xerox® Device Manager to use non-default community string names and to use multiple community string names. Be careful when configuring additional community string names because each name increases the overall discovery process workload.

SNMP V3 SECURITY ENHANCEMENTS

SNMP is the most widely used in-band management protocol used for communication among network management stations and the devices being managed. In its current form, SNMP's security is limited to three methods of access: Read-only, Write-only and Read-write. Access from the management station (Xerox® Device Manager) to the devices is granted by "community strings," which are simply the groups to which the devices belong. Although disabling the write function in SNMP can prevent most in-band attacks, SNMP is a relatively insecure protocol, with nothing more than the community strings acting as passwords.

The SNMP V3 framework supports multiple security models, which can exist simultaneously, within an SNMP entity. SNMP V3 messages contain a field in the header that identifies which security model must process the message. To ensure some form of interoperability, a User-based Security Model (USM) is implemented to defend against unauthorized modification of managed elements and spoofing. Although SNMP V3 is a huge step forward in secure manageability, it cannot prevent "denial-of-service" attacks. In addition, its security system must stand alone, meaning every device must have a database of users/passwords. Since this is not likely to happen in most companies, all devices are left at risk.

Users and Groups

Xerox® Device Manager provides access restriction based upon the roles assigned to Windows users including: Administrator, Power User, and User. The **Administrator** role is used during the Xerox® Device Manager installation and remote discovery procedures, **Power User** during print management activity, and the **User** role for local discovery, view-only display and reporting.

Note: User names and passwords are not sent over the network. If no username is provided during software installation, the Xerox® Device Manager installer will create a "CWW Run As Account" user and place it into the local Administrators group. If a username is provided at installation, that user will be authenticated and then placed in the local Administrators group. If users remain restricted to the local Administrators group, they will only be able to manage local printers and queues and not be able to manage any network connected devices.

CWW-SPECIFIC GROUPS

Access restriction is dependent upon the groups to which the user is assigned. Xerox® Device Manager creates user groups during install that grant members specific rights to the Xerox® Device Manager application. Xerox® Device Manager groups are created with "CWW" in the name.

The **CWW Administrators** group grants full administrative permissions to its members.

The **CWW Power Users** Group grants print management permissions to users in environments where sysadmin privileges would be neither required nor desirable. Members of this group can:

- Create/Edit/Delete reports
- Edit and Modify Traps

- Edit Printer/Protocol/Scan Properties printer action
- Apply Configuration Sets/Check Compliance
- Troubleshoot/Reboot faulted printers
- Perform printer group administration

The **CWW Configuration Set Admin** performs all actions on configuration sets and may edit printers, troubleshoot, and reset printers.

The **CWW Edit Device Admin** may edit printers, troubleshoot, run configuration sets, and reset printers.

The **CWW Report User** has limited access to the Reports tab and may view and send reports.

The **CWW Report Admin** may perform all action on reports.

The **CWW SQL Users Group** grants rights to run the Xerox® Device Manager application instead of using the Network Services account.

The **CWW Customer Group** grants access rights to the Xerox® Device Manager Customer View.

The **CWW Customer Administrators Group** grants administrative rights to access the Xerox® Device Manager Customer View.

The **CWW User** may view the printer group to which the user belongs, refresh printer data, and view the Xerox® Services Manager asset details for a printer.

The **CWW Customer Report User** has read access to the device compliance dashboard and includes the permissions of the CWW Customer. Users cannot remediate or create policies, they can only see the results.

The Run As Account

Before deploying Xerox® Device Manager, the implementation team should consider whether there is a need to administer remote print servers. If there is a need, then the necessary authorization credentials for those print servers are required. Xerox® Device Manager supplies an existing account as the application administrator. The Run As capability provides additional security by defining a specific Windows® account that Xerox® Device Manager can use to administer print servers. Enter these credentials in one of the following ways:

- The application installer provides an input for the Run As account, if known.
- The Xerox® Device Manager Configuration Utility specifies the credentials of the Run As account after installation. This utility complies with the customer user account security policies and provides flexible configuration of the Xerox® Device Manager application.
 - The Xerox® Device Manager Configuration Utility can only be launched from the Xerox® Device Manager server UI unless Terminal Services are available.
 - The Xerox® Device Manager Configuration Utility is accessed from Start>Programs>Xerox on the Xerox® Device Manager server. This utility enables an administrator to perform the following tasks:
 - Change the default Xerox® CentreWare® Web user account password
 - Change the password of the Run As account
 - Change the password of the SQL Server and port
 - Import and export databases

Required Permissions

Depending on the configuration of the devices that need to be managed, you might need different levels of accounts and privileges. The table below outlines the functions and privileges required within Xerox® Device Manager and offers some alternate group choices to accomplish printer and queue management.

Xerox® Device Manager Function	Required Privileges for the Xerox® Device Manager Run-As Account
Discover Network Printers	None
Discover Locally-connected (Direct) Desktop Printers	Account can be a member of the Domain Users group to query only shared print queues on every computer that will be inspected or Member of the Domain Administrators group to query both shared and unshared print queues on every computer that will be inspected or Member of every computer's local Administrators group to query both shared and unshared print queues on every computer that will be inspected Note: Integration with XPA for the detection of Locally (Direct) Printers does not require certain permissions from the Run As Account.
Discover Computers	Member of the Domain Users group to discover and retrieve only basic computer properties or Member of the Domain Administrators group to discover and retrieve basic AND detailed computer properties or Member of every computer's local Administrators group to discover and retrieve basic and detailed computer properties
Discover printers via Active Directory® partitions	Member of the Domain Users group
Discover printers via Managed Print Servers	Account can be a member of the Domain Users group to query only shared print queues or Member of the Domain Administrators group to query both shared and unshared print queues or Member of every computer's local Administrators group to query both shared and unshared print queues
Create New Queue + Publish in Active Directory	Member of the local Administrators group where print queue is created
Delete/Edit Print Queue	Member of the Print Operator group or Member of the Administrators group where the queue resides
Certificate Management	In order to access the private key to download the certificate from an NDES server security, a Network Service user needs security permission in the following folder: C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys

Xerox® Device Manager Run As Account Privileges

Windows Considerations

You may want to disable Internet Explorer Enhanced Security Configuration. This improves user experience.

1. To disable this feature click on **Start > Administrative Tools > Server Manager**.
2. Under Security Information select **Configure IE ESC**.
3. The Have Disk control for adding device drivers to the print server in Xerox® Device Manager will not work unless webdav has been enabled for IIS.
4. To enable webdav for IIS, select **Start > Administrative Tools > Internet Information Services (IIS) Manager**. Click on **Web Service Extensions** and then select **Webdav** in the right pane. Finally, click the **Allow** button.

Printer Information Communicated to Xerox® Services Manager

The table below identifies printer attributes exported by default to Xerox® Services Manager. In those account implementations where customer network security may dictate limited data exports, all of these fields (except for those in the bulleted list below) can be disabled for transmission to Xerox® Services Manager through the Account Administration>Field Customization function within Xerox® Services Manager.

- Description
- Icon
- Manufacturer (Device)
- Serial Number (Device)
- Serial Number (Scrubbed)
- Usages Counter Meters

Once configured, Xerox® Services Manager communicates these restrictions to Xerox® Device Manager to prevent transmission of restricted data by Xerox® Device Manager to Xerox® Services Manager. For those accounts requiring configuration of fields in Xerox® Device Manager, a subset of these fields can be configured within the Xerox® Device Manager server's Xerox Services Manager sync options configuration. The list of fields disabled in Xerox® Device Manager can be seen in Xerox® Services Manager, but cannot be modified within Xerox® Services Manager.

2 Sided Percentage	Advanced Finishing Supported	Advanced Status Update Date	Analog Fax Capable
Analog Fax Description	Analog Fax Modem Installed	Analog Fax Phone Number	Black Rated PPM
Can Manage	Color Capable	Color Rated PPM	Compliance Level
Console Country	Console Language	Customer Asset Number*	Custom Property 1
Custom Property 2	Custom Property 3	Custom Property 4	Custom Property 5
IP Default Gateway	Description*	Device Language	Device Time Zone
Discovery Date	Discovery Method	Discovery Type	DNS Name
Duplex Capable	Finishing Options	Firmware Level*	Hard Disk Present
Hard Disk Size MD	Icon	IP Address Changed	IP Address (Device)
IPX Address	IPX External Network Number	IPX Print Server Name	Last Known IP Address
Last Status Attempt	MAC Address Machine Up	Main Status	Manage Request Date

	Time		
Manage Request Date	Managed State	Manufacturer (Device)*	Marking Technology (Device)
Xerox Asset Number	MIB Country	Physical Memory Total MB	Queue Name (Device)*
Scan to E-Mail Capable	Scan to File Capable	Scan to Internet Fax Capable	Scan to Server Fax Capable
Scanner Description	Scanner Installed	Serial Number (Device)*	Serial Number Scrubbed
Status Date	SubnetAddress	Subnet Mask	System Contact
System Name	Target Volume	Traps Enabled	Traps Supported
Type*	Update Date	Usage Counter (Meters)*	Utilization Percentage
Consumables Information			

Printer Fields Exported to Xerox® Services Manager by Xerox® Device Manager

Note: Items marked with an * are items sent for Locally Connected (Direct) Printers.

XEROX® DEVICE MANAGER SERVER INFORMATION EXPORTED TO XEROX® SERVICES MANAGER

Certain fields are required by Xerox® Services Manager in order to successfully export job accounting data up to Xerox® Services Manager. Please note that you should enable or disable any optional fields in Xerox® Device Manager before enabling the feature that will export job accounting data to Xerox® Services Manager.

Xerox® Device Manager Server DNS Name	Xerox® Device Manager Server IP Address	Xerox® Device Manager Site Name	Xerox® Device Manager Software Build version
Xerox® Device Manager Server Time Zone	License Expiration Date	Xerox® Device Manager database size (in MB)	Xerox® Device Manager Discovery database size (in MB)
Hard Drive capacity (in MB)	Hard Drive free space (in MB)	Xerox® Device Manager Server RAM memory size (in MB)	Xerox® Device Manager Server RAM memory free size (in MB)
Number of Managed Printers	Number of Unmanaged Printers	Critical Services running on the Xerox® Services Manager Server (this includes both Xerox® Device Manager and Xerox® Services Manager)	Operating System Name
Operating System Type (32/64 bit)	Processor	.NET version	Corporation Security Mode
Xerox® Device Manager Server MAC Address (Current & Initial)			

Xerox® Device Manager Information Exported to Xerox® Services Manager

XEROX® DEVICE MANAGER JOB ACCOUNTING DATA EXPORTED TO XEROX® SERVICES MANAGER

Certain fields are required by Xerox® Services Manager in order to successfully export job accounting data up to Xerox® Services Manager. Please note that you should enable or disable any optional fields in Xerox® Device Manager before enabling the feature that will export job accounting data to Xerox® Services Manager.

Column Name	Required	Enabled by Default	Description	Comments
j_clientMachineName	No	Yes	WINS name of workstation from where job was submitted	
j_colorPrint	No	Yes	Whether job is color	
j_contentSize	No	Yes	Job size in bytes	
j_copiesPrinted	No	Yes	Number of copies requested for the job	
j_deviceIP	No	No	IP address of the printer that processed the job	Not exported
j_deviceMACAddress	No	Yes	Mac address of the printer that processed the job	Not exported
j_deviceModel	No	No	Printer driver through which the print job was submitted	Not exported
j_documentName	No	Yes	Title of the job	
j_documentTypeID	No	Yes	Document type of the file which was submitted as a print job	
j_duplexPrint	No	Yes	Whether job requested is duplex	
j_jobCompletionTime	Yes	No	Date and time when the job is completed as per the job reporting source	
j_jobID	Yes	No	Job ID assigned by the source reporting the job	
j_jobPK	Yes	No	DB Unique ID assigned to each job record	
j_jobSubmissionTime	Yes	Yes	Date and time when the job was submitted as per the job reporting source	
j_mediaSize	No	Yes	Media size requested in the job	
j_mediaType	No	Yes	Media type requested in the job	
j_ownerUser	No	No	Network user who submitted the job	
j_pageCount	No	Yes	Total impressions scanned or printed by the printer	
j_printServerName	No	Yes	WINS name of the machine that delivered the job to the printer	
j_queueName	No	Yes	Windows Queue Name through which job was printed	
j_portName	No	Yes	Windows Queue Port Name through which job was printed	

Column Name	Required	Enabled by Default	Description	Comments
			ted	
j_printServerMacAddress	No	Yes	Mac address of the machine that delivered the job to the printer	
j_overflowOccured	No	No	Set to TRUE if Xerox® Device Manager determines erroneous page count was reported	Not exported
j_exportedXAM	No	No	Set to TRUE if job record has been exported to Xerox® Services Manager	Not exported
j_uniqueID	Yes	No	Unique ID of the printer record that processed the job	
j_deviceCreated	No	No	Set to TRUE if job associated printer is known to Xerox® Device Manager	Not exported
j_bwPageCount	No	Yes	Total BW impressions scanned or printed by the printer	
j_colorPageCount	No	Yes	Total Color impressions scanned or printed by the printer	
j_jobType	Yes	Yes	Whether the job is PRINT or COPY or SCAN or FAX-SEND or FAX-RECEIVE	Required
j_jobAcctSource	No	Yes	Identifies the job accounting source: blueprint, equitrac, docusp, other	Added
j_devJobCompletionTime	No	Yes	The job completion time reported by device.	Added
j_userID	No	Yes	The accounting user name	Added
j_userAccountID	No	Yes	The chargeback code for the job	Added
J_deviceDNSName	No	Yes	DNS Name of the printer	
J_deviceSerialNumber	No	No	Serial Number of the printer	
j_jobUniqueID	No	Yes	The unique job ID	Added
j_chargebackPrice	No	Yes	The chargeback price of the job	Added

Column Name	Required	Enabled by Default	Description	Comments
j_colorMode	No	Yes	The job color details: 1 color, 2 colors, 3 colors, 4 colors, few colors, auto, for low price mode, mixed, monochrome, other, unspecified	Added
j_nUp	No	No	Number of images per page	Added. Only exported for FX.

Xerox® Device Manager Job Data Exported to Xerox® Services Manager

XEROX® DEVICE MANAGER POLICY LOG DATA EXPORTED TO XEROX® SERVICES MANAGER

If XPA is leveraged in the account to implement the Enterprise Print Governance solution, policy log data is collected by Xerox® Device Manager and then exported to Xerox® Services Manager. The following log data is collected as per policy violation when a print document is submitted:

Client Machine Name	Print Server Name	Date and Time when policy rule was violate	Document Name
Windows Network User Name	Windows Print Queue Name	Rule Action	Is Customer Notified
Is Duplex	Is Color	Total Impressions	Job Price
Message shown to the User	Print Policy Plan Name	Print Policy Rule Name	

NEW ENTRY

CORPORATE SECURITY MODE

In addition to any scheduled synchronization by the Xerox® Device Manager server to Xerox® Services Manager, there is a daily synchronization performed by default. If all scheduled synchronizations are turned off, the daily synchronization maintains accurate information between Xerox® Device Manager and Xerox® Services Manager. There is a capability within Xerox® Device Manager to turn off this daily synchronization. Within the **Administration > XOS Suite > Xerox Services Manager > Sync Option** page, there is a configuration item for Corporation Security mode. The two modes that exist are **Normal** and **Locked Down**. In Normal mode, the default synchronization will continue to run when all scheduled synchronizations have been switched off (recommended mode). In Locked Down mode, the default synchronization will also be turned off if all polling schedules are switched off as well. When Locked Down mode is turned on, there is no communication with Xerox® Services Manager, and any setting changes done through Xerox® Services Manager must then be done on-site. Locked Down mode does the following:

1. Disable the Nightly synchronization with Xerox® Services Manager.
2. Disables the sending of the Xerox® Device Manager server IP address and DNS name to Xerox® Services Manager.
3. Disables the sending of device IP address information to Xerox® Services Manager.
4. Disables the ability to import Xerox® Services Manager discoveries.
5. Disables the export of Xerox® Device Manager discoveries to Xerox® Services Manager.

REMOTE COMMANDS FROM XEROX® SERVICES MANAGER

Xerox® Device Manager can be configured in two ways to check its corresponding account within Xerox® Services Manager to see if the account administrator has posted a command request to Xerox® Device Manager.

First, Xerox® Device Manager can be configured for instant remote commands. When configured for instant remote commands, Xerox® Device Manager will make an immediate connection to Xerox® Services Manager for remote commands. Xerox® Services Manager will not return and the session will be left open until a command is posted or the session is timed out. When a command is posted, Xerox® Device Manager will execute the command and return to Xerox® Services Manager with the results, and then reopen a new session. If there is a timeout a new session will be established with Xerox® Services Manager within 60 seconds. In this configuration, we can get real-time responses to commands, reducing the time operations centers wait for information.

Second, Xerox® Device Manager can be configured to periodically poll. You can configure Xerox® Device Manager to periodically poll its corresponding account within Xerox® Services Manager to see if the account administrator has posted a command request to Xerox® Device Manager. This polling is an extremely lightweight Web interface interrogation by Xerox® Device Manager and should cause little if any extra network bandwidth loading for the customer's IT network. Both configurations use standard HTTPS port 443 on an inbound to Xerox® Device Manager basis.

The list of commands available to an Xerox® Services Manager account manager to request is the following:

- **Get Device Status** – obtains the current status of a device.
- **Reboot Device** – stops and restarts a device.
- **Troubleshoot Device** – pings a device and retrieves its status.
- **Upgrade Device** – updates the device to a newer software release version.
- **Start Managing Device** – sets the status of the selected device to the managed state. When a device is in the managed state, device data, such as meter readings and alerts, are sent to the application.
- **Print Test Page** – initiates a test print job on a device.

Xerox® Device Manager can disable access to each of the Xerox® Services Manager remote commands during setup of the Xerox® Device Manager Xerox® Services Manager Configuration. This includes Device Remote Commands as well as Remote Configuration commands.

REMOTE CONFIGURATION

The list of commands available to an Xerox® Services Manager Account Manager to request is the following:

Device Discovery	Xerox® Services Manager can issue a request for a specific IP Sweep discovery, which can include individual IP addresses, IP address ranges, and lists of subnets. The definition for the IP Sweep specified by Xerox® Services Manager is stored within Xerox® Device Manager locally within its built-in Xerox Services Manager Sweep . Using the results of this sweep, Xerox® Device Manager will automatically upload any new discovered device information and a results summary, so that the Xerox® Services Manager account manager can review it.
Rediscovery	You can configure the Rediscovery within Xerox® Device Manager from Xerox® Services Manager. This discovery method refreshes all the printer information for each device known by Xerox® Device Manager. You can configure the time when this discovery runs, the number of retries, and the timeout period.

Data Export	Within Xerox® Services Manager, you can configure when the managed and unmanaged devices are exported to Xerox® Services Manager. You can change these settings for each Xerox® Device Manager server found in an account from Device Manager>Data Export page.
Network Settings	You can use Xerox® Services Manager to change the following key settings within Xerox® Device Manager: the default number of retries and timeout, how often to retrieve status from both managed and unmanaged devices, and the SNMP set and get community strings names that are used when communicating to a device.
Unlink and Delete Device	You can use Xerox® Services Manager to unlink and delete a device from the Xerox® Device Manager database. In this way, you can remove a device from the Xerox® Device Manager database so that it is not reported to Xerox® Services Manager. If the device is rediscovered, it will be added back into the Xerox® Device Manager database resent back to Xerox® Services Manager.

Xerox® Services Manager-Initiated Remote Configuration

ADDITIONAL ADMINISTRATION CAPABILITIES

Xerox® Device Manager Circuit Breaker Configuration Settings

Any (and all) of the Xerox® Device Manager related net-based functions can be quickly disabled without application reconfiguration via the **Admin > Network > Network Usage Configuration > Application Wide Network Traffic Switch** dialog. This feature makes it easy to switch off network traffic generated by Xerox® Device Manager during troubleshooting or evaluation.

Xerox® Device Manager Logs

Action Log

This log enables you to view all actions that occur during administration of the application. It can be used to track unauthorized changes to the application or to provide a process log of activity. The log displays the Category and Subcategory where the activity was performed, the user who performed the activity and the time and date of the activity are shown.

Audit Log

This page enables the user to view a log that tracks changes made to critical areas of the Xerox® Device Manager server application. The Audit log tracks who made the changes, as well as what was changed. Critical areas include Discovery Setups, Xerox® Services Manager settings, Discovery exclusions, and Status polling configuration.

An additional set of audit logs (XDM Audit Log) is available through the Windows Event Viewer. These logs allow users to ascertain the security level being maintained, and they provide forensics data in case of a security issue. The XDM Audit Log is in XML format and contains Event IDs that reflect the source of the logged event/function.

E-mail Log

This page enables the user to view all E-Mails sent out by the Xerox® Device Manager application. The Log contains information pertaining to the recipients of the email, the date and time of email, the subject, the application source, and the email message body.

Event Log

This page enables the user to view the print server's event log, particularly informational and error messages. The type of event, date, source, category, and identity information is shown. Click **Refresh** to update the information on this page.

Systems Infrastructure

Network Ports Used by Xerox® Device Manager

Xerox® Device Manager relies on a number of TCP/IP network ports, all predefined by the Windows® operating system as defaults to perform its activities. A table of Xerox® Device Manager features, network protocols, and ports with the data direction (related to the Xerox® Device Manager server) is defined below.

Xerox® Device Manager Feature/Function	Protocol	Port Number Used	Data Direction
Xerox® Device Manager Web page queries Job accounting data Auto Driver Download Cloning Wizard Scan Template configuration set transfer Troubleshoot Xerox® Print Agent Communications Configuration Sets	HTTP	80 but could be altered via IIS Administration	Incoming/Outgoing
Secure Xerox® Device Manager Web page queries Secure Xerox® Device Manager-to-Hosted data transfer Upgrading Android Tablets	HTTPS	443	Incoming/Outgoing
Receive unsolicited printer status notifications	SNMP v1 Trap	162	Incoming
Network printer discovery using Novell® Server queries via IPX	SAP	452	Incoming
Network printer discovery Retrieval of capabilities, status & usage counters Single device configuration Configuration sets	SNMP V1, V3 SNMP V1, V3	161 but could vary depending upon OS port allocation 161	Outgoing/Incoming Incoming/Outgoing
E-mail alerts	SMTP	25	Outgoing
Printer discovery via Managed Server/Active Directory Queue-based operations/diagnostics Locally-Connected Printer discovery Data synchronization	RPC	135	Outgoing
Retrieval of computer properties	WMI over RPC	135 + random port	Outgoing
Network printer discovery for non-SNMP-enabled printers	IPP	631	Outgoing
Add/Delete Directory Scan Service Configuration Set Active Directory Customer Import Customer Group Configurations	LDAP	389	Outgoing
Troubleshoot – Print Test Page Printer Firmware Upgrade	TCP/IP	515, 9100, 2000, 2105	Outgoing

Xerox® Device Manager Feature/Function	Protocol	Port Number Used	Data Direction
Managed Print Server Xerox® Print Agent operations Computer property queries	NetBIOS	137, 139	Outgoing
Xerox® Print Agent operations	SMB	445	Outgoing
Xerox® Print Agent communications	WCF	23900	Outgoing
Network Printer Discovery Troubleshoot / [Test]	PING / CMP	none	Outgoing
Hard coded for Remote Discovery	TCP	8105	Internal Xerox® Device Manager uses to communicate with Scheduler
Scheduler (Changeable string entry in the registry)	TCP	8085	Internal Xerox® Device Manager uses to communicate with Scheduler
Reverse DNS Lookup of discovered devices	DNS	53	Outgoing

Ports and Protocols Used by Xerox® Device Manager

Note: Some customer environments may restrict the routing of ICMP packets across routers using an access control list to avoid denial of service attacks and worms (e.g., Nachi) from impacting their network. As a result, the following Xerox® Device Manager features will be adversely impacted:

- Troubleshoot Printers wizard
- Troubleshoot within Printers device view
- Add Printer within Printers device view
- IP Domain Scan for computers within the Discovery Administration tab
- Add Server within Queues device view

Windows® Services Utilized by Xerox® Device Manager

The following Windows-based services are part of or are used by the Xerox® Device Manager application:

- Internet Information Service (IIS)
- Windows® Print Spooler
- Remote Procedure Calls
- Windows® Management Instrumentation (for detailed computer information)
- SQL Server® Service

The following services are part of the Xerox® Device Manager application. These services will automatically start when the system boots and will restart if stopped:

- Xerox Discovery Service (device discovery and identification and SNMP trap monitoring)
- Xerox Scheduler Service (automatic and scheduled background tasks, e.g. device polling, discovery)

GENERAL DISCOVERY CONSIDERATIONS

The Discovery function allows Xerox® Device Manager to search for network printers on the customer's intranet. Device discovery is a crucial part of the Xerox® Device Manager application because it is the main method to identify networked and direct-connected devices and store them in the database. It is a compound operation that involves discovering appropriate network addresses based on the type of discovery configured and the subsequent querying of those addresses (via SNMP) for device type and

general configuration information. Since this operation uses the network resource, consider what information you want to be detected and configure the discovery to achieve this goal with a minimum of network contention. Xerox® Device Manager provides a number of customizable methods to discover devices and various ways to manage discovery to gain the most information with the least impact to network bandwidth.

Managing Discovery

The discovery process can be managed in a number of ways.

- You can set up discovery to only discover those devices in certain locations. This throttling ability can be used to customize the discovery processes and reduce the amount of network traffic generated by Xerox® Device Manager.
- You can schedule discoveries to execute during off-hours to reduce impact to network traffic.
- You can set up the Xerox® Device Manager server to execute multiple instances of discoveries. Each discovery instance can be saved.
- You can add exclusions to Xerox® Device Manager to limit or specify the IP subnets and addresses that will not be probed.
- You can control the discovery process by the use of SNMP community name strings to query certain network printers over others.
- You can retrieve status information since the discovery will provide active status on its progress, the number and types of devices found, and information about the last scan, including how long it took to complete.
- You can establish device timeout and retry parameters before the discovery occurs to get print information from slower network subnets on a WAN.
- Xerox® Device Manager can import discovery parameters from CSV files, at the time of creation or when the discovery runs, to eliminate tedious data entry. This import capability also provides CSV file error handling and duplicate address checking, which reduces the amount of time required to configure Xerox® Device Manager.

Printer Rediscovery

Xerox® Device Manager also provides a printer rediscovery capability, which will gather information about previously discovered printers. You can schedule rediscovery to query for any changes to only those devices contained within the database (e.g., firmware level, scan-to-e-mail capability, physical memory, etc.).

Note: When the initial discovery was an SNMP v3 sweep and the devices are then enabled for v1/v2, if the rediscovery is an SNMP v1 or v2 IP sweep, the devices will not be discovered. To discover those devices, the user must first clear the devices from the database in Xerox® Device Manager and perform an SNMP v1/v2 IP sweep again.

This capability helps when monitoring for device changes and is also used to cut down on the number of new discoveries needed, thus reducing network bandwidth requirements.

Note: As a rule of thumb, each printer that is discovered may generate as much as 50KB (maximum) of network message traffic including device capabilities, usage counters, and an alert table.

IP Sweep Discovery

Operation

The IP Sweep Discovery method is the preferred method of accurately discovering printers on a network (see the Alternative Device Discovery Methods section for the other discovery methods available in Xerox® Device Manager). A packet is sent to every IP address within the user-defined subnet or address range list. These address ranges should be known and provided before running the discovery.

Specifically:

- A single packet is sent to each IP address contained within each subnet or address range defined within the current IP address for the current IP Sweep. In this packet, Xerox® Device Manager requests a value for a single SNMP-based RFC 1213 Object Identifier (OID).
- For each device that responds to the RFC 1213 OID, Xerox® Device Manager will add the IP address of the response packet into its list of live IP addresses.
- Xerox® Device Manager then queries those devices with live IP addresses for two more OIDs: one RFC 1213 OID and one RFC 1759 OID. This enables Xerox® Device Manager to identify printing devices from non-printing devices. Both groups of devices are stored within the Xerox® Device Manager database, however, only printing devices are exposed via the Xerox® Device Manager UI.
- For those printer devices that respond to the RFC 1759 OID query, Xerox® Device Manager flags them as printers.

For those devices that do not respond to the RFC 1759 OID query, Xerox® Device Manager then checks a RFC 1213 OID value against two registry key values to determine if the device is in fact a known printer. This is necessary because some printing devices (e.g., printers using external print server boxes, older printers, etc.) do not support RFC 1759 – the Printer MIB.

The registry keys contain RFC 1213 values for several known supported and unsupported printers.

- Xerox® Device Manager then queries all live IP addresses for three RFC 1213 OIDs and one RFC 1514/2790 OID.
- For those devices identified as printers, Xerox® Device Manager queries three more RFC 1514/2790 OIDs and four more RFC 1759 OIDs to obtain some basic attributes of the printer
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID and a new OID from the Internet Draft of the Printer MIB in order to obtain the printer's serial number.
- Xerox® Device Manager then queries 3 RFC 1759 OIDs in order to display the printing device's rated speed in pages per minute units (PPM).
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID(s) to obtain the printing device's software/firmware level.

Note: Before implementing the IP Sweep method, the evaluator must be supplied with a list of known IP addresses (and subnet ranges) to use. By preconfiguring the subnet and IP address information, you can tailor discovery to find or exclude specific subnets or groups of printers.

When to Use

The IP Sweep Discovery method is the preferred method of accurately discovering printers on a network. Use this method when the client has knowledge of the IP subnet addresses where printers may exist.

Network Impact

The amount of network traffic generated by a sweep-based discovery is minimized because the requests are directed to specific IP addresses.

Accuracy

The IP Sweep method produces a controlled and orderly flow of data between the printers and the server, reducing network packet collisions that can introduce errors in the printer information.

DISCOVERY NETWORK DATA CALCULATIONS

As mentioned earlier, each discovered printer can create as much as 50KB of discovery-based traffic. IP Sweep discovery sweeps all of the addresses in the ranges supplied.

Device Discovery Data Set Magnitudes On Typical Printers

The amount of data transferred during an operation, such as discovery or status polling, is a function of the device's capabilities. Measurements made on typical devices show the variability of these parameters. It is highly unlikely that any one network would be populated with only one device type. Instead, the typical case is a variety of devices that are dependent upon the particular needs of individuals or groups on the network. Here are three printer examples to demonstrate the variability in both the amount of collected data and the data transfer rate for typical devices.

As we release new and updated machines with increasing functionality, the size of the discovery dataset will also increase. The network traffic volume may be higher for machines and sites with more advanced technology.

Machine Model	Discovery	Historical Data Gathering	Status Polling
Xerox® WorkCentre® 7800	263 KB	15 KB	1.0 KB
Xerox® WorkCentre® 3315	116 KB	7 KB	1.1 KB
VersaLink® 7035	133 KB	13 KB	1.2 KB
Xerox® Phaser® 4622	115 KB	6 KB	1.0 KB
AltaLink® C8055	261 KB	8 KB	1.2 KB
AltaLink® C8070	180 KB	20 KB	1.3 KB
CERT avg	178KB	11 KB	1 KB

Typical Device Data

You also need to consider the frequency at which you will perform these operations. For purposes of this document, the following schedule for device data retrieval and their data set size will be assumed to be:

Operation Type	Frequency	Average Data Set Size
Discovery	Weekly	178 KB
Historical Data Gathering	Never	11 KB
Status Polling	Hourly	1 KB

Xerox® Device Manager Data Gathering Options

It will be assumed that:

- Xerox® Device Manager will discover and monitor 1000 network devices,
- Xerox® Device Manager does not perform historical data gathering,
- Xerox® Device Manager is configured for communication to a hosted site.

Each device discovery data set size is 178KB, its historical data gathering set size is 11 KB, and its status polling data set size is approximately 1 KB.

This set of devices is expected to retrieve the following printer-based discovery data over the network each month:

- 4 discovery cycles/month x 1000 printers x 178KBytes/printer (Discovery data set size) is approximately 712MB/month

Note: Extended Data Retrieval, when enabled, will increase the amount of data retrieved from a device. Extended Data Retrieval gathers the data related to protocol information (see the Protocol tab on the

Device page) on a polling basis for the purposes of reporting changes within the Change History report. The data set size is less than that of a full Discovery.

Network Impact Considerations of Status Polling

Xerox® Device Manager communicates with the printers under management on a regular basis. Examples include status polling and historical data gathering (scheduled to run at certain times) and SNMP traps (occurring at random times). Each transaction consists of a series of back-and-forth SNMP queries with the device, beginning with an are you there query, then progressively asking for more information (with each device response) until the transaction purpose is complete.

SCHEDULED COMMUNICATIONS CALCULATIONS

Status polling assumptions:

- Status polling traffic averages 1 KB per transmission
- Status polling occurs every day, once per hour (24x7)
- 1,000 printers are being monitored

The expected amount of data to be retrieved from this set of devices over the network for printer-based discovery over one month is:

1,000 printers x 24 hours x 30 days x 1 KBytes is approximately .72 GB per month

Scheduled Status Retrieval And Alerts Feature

Xerox® Device Manager restricts the hours of operation when it will retrieve printer status and alerts polling. By defining a schedule within Xerox® Device Manager, status retrieval will occur only during certain hours for each week.

SNMP ALERTS TRAFFIC CALCULATION

An SNMP trap is an unsolicited alert that notifies Xerox® Device Manager when a significant event occurs on a network device. Traps can occur at any time and have minimal impact on network traffic (packet size is approximately 1KB). Xerox® Device Manager allows you to configure which events in a device warrant trap notification and supports a feature called Intelligent Trap Reception. You can configure this feature to either perform a status query to the device immediately after receiving a trap, or to collect traps for 30 seconds before querying the device generating the fault. This 30-second time delay eliminates unnecessary queries to devices, which reduces network traffic.

SNMP Trap Assumptions:

- Intelligent Trap Reception is set to query immediately after a trap occurs
- 1,000 devices are monitored
- 20% of the devices generate a trap during one month

The calculation for the amount of net traffic generated during a month of SNMP traps is: (1 KBytes per trap packet + 15 KBytes per query) x 200 device traps = 3000KB or ≈ 3 MB/mo.

Note: With trap support enabled, you can consider a reduction in the frequency of status polling, which can be a great benefit to both the customer network bandwidth considerations as well as proactive device monitoring goals.

Active Directory® Customer Import Network Data Calculations

Xerox® Device Manager can be configured for periodic synchronization of customer data from Active Directory. You can configure which fields need to be synched. At the most, each customer import generates ~2KB of network traffic, which includes data and AD interfaces overhead.

Total Xerox® Device Manager Data Transfer Calculations

The next two traffic calculation examples show totals for both a typical and a more exaggerated network data transfer size during a one-month period. Both totals include the use of regularly scheduled discovery, status polling, historical data gathering, and job tracking activities.

The first example estimates traffic based on the typical sizes of network communications used by Xerox® Device Manager. This also assumes Xerox® Device Manager is configured to business hours of 8 hours/day and 21 days/month. Using 178KB for discovery, 1KB for non-printers, 1KB for status polling, and 11KB for historical data gathering, and 4KB for Xerox Print Agent, the network traffic could be as much as follows for the same 1,000 printers in a given month:

Discovery total

$2 \text{ cycles/month} \times 1,000 \text{ printers} \times 178 \text{ KBytes /printer} = 60,000 \text{ KB/month} \approx 356 \text{ MB/month}$

Discovery traffic to non-print devices during a sweep

$2 \text{ cycles/month} \times 1000 \text{ IP Address} \times 1 \text{ KBytes/packet} = 2,000 \text{ KB/month} \approx 2 \text{ MB/month}$

Historical Data Gathering total

$21 \text{ days/month} \times 1,000 \text{ printers} \times 11 \text{ KBytes/printer} = 231,000 \text{ KB/month} \approx 231 \text{ MB/month}$

Status polling total

$21 \text{ days/mo} \times 8 \text{ polls/day} \times 1,000 \text{ printers} \times 1 \text{ KBytes/printer} = 168,000 \text{ KB/month} \approx 168 \text{ MB/month}$

*Job Tracking total

$21 \text{ days/mo} \times 15 \text{ print jobs/day} \times 1,000 \text{ users} \times 4 \text{ KBytes/job} = 1,260,000 \text{ KB/month} = 1.20 \text{ GB/month}$

OVERALL (Typical) TOTAL

$356 \text{ MB} + 2 \text{ MB} + 231 \text{ MB} + 168 \text{ MB} + 1.20 \text{ GB} \approx 1.9 \text{ GB/month}$

The second calculation is inflated to show an above-the-limits traffic estimate. It assumes that every discovery requires 200 KB of traffic to complete (except non-printer discovery); history requires 20 KB; status requires 10 KB; and that the organization is active 30 days per month. Although this situation is extremely unlikely, it demonstrates the extreme upper limits for a network with 1,000 print devices being monitored monthly.

Discovery total

4 cycles/month x 1,000 printers x 200KBytes/printer = 800,000 KB \approx 0.8 GB/month

Discovery traffic to non-print devices during a sweep

4 cycles/month x 65,534 IP Address x 1 KBytes/device = 262,136 KB \approx 0.250 GB/month

Historical Data Gathering total

30 days/month x 1,000 printers x 20 KBytes/printer = 600,000 KB \approx 0.6 GB/month

Status polling total

30 days x 24 polls/day x 1,000 printers x 10 KBytes/printer = 7,200,000 KB/month \approx 7.2 GB/month

***Job Tracking total**

30 days x 15 print jobs/day x 1000 users x 7 KBytes/job = 3,150,000 KB/month \approx 3.0 GB /month

AD Customer import total

30 days x 10000 users x 2KBytes/user = 300,000 KB/month \approx 0.6 GB /month

OVERALL (Exaggerated) TOTAL

0.8 GB + 0.250 GB + 0.6 GB + 7.2 GB + 3.0 GB + 0.6 GB \approx 12.45 GB/month

*Job Tracking calculations shown above are based on legacy Job Tracking Agent (JTA) software. JTA is superseded by Xerox Print Agent, which may generate higher network traffic depending on what features are being used. Please refer to the XPA Certification guide for the exact details on network traffic generated due to XPA and Xerox® Device Manager communication.

EMAIL DATA COMPARISON

The following e-mail example can be used as a comparison to the amount of traffic generated by Xerox® Device Manager. Assume an average size of 3 KB (essentially text-only) with 1,000 employees using e-mail 20 times per day every business day a month.

E-mail Data - Assuming 3KB average size

21 days/month x 20 e-mails/person x 3 KBytes/e-mail x 1,000 person = 1,260,000 KB/month \approx 1.20 GB of E-mail Data/month

The example above is based on text-only e-mails and demonstrates the lower end of traffic. It does not include any attachments to e-mail traffic that are typical. Therefore, the above estimate could be an order of magnitude less than what could be experienced on the same 1,000-employee network that includes attachments. The following e-mail example contains the same calculation based on a size of 30 KB (assuming a 27KB attachment).

E-mail Data - Assuming 30KB average size

21 days/mo. x 20 e-mails/person x 30 KBytes/e-mail x 1,000 person = 12,600,000 KB/month \approx 12 GB E-mail data/month

Note: Although it is difficult to accurately determine the amount of network traffic generated and consumed by an application like Xerox® Device Manager (and/or e-mail) with all of its options and activity, the above comparison proposes that the Xerox® Device Manager data created and transferred across the network is significantly lower than that created and consumed by even a conservative e-mail implementation.

Production Device Job Data Transfer

For production-based devices, Xerox® Device Manager retrieves job data for accounting purposes using IPP. This table shows the approximate amount of data transferred per job:

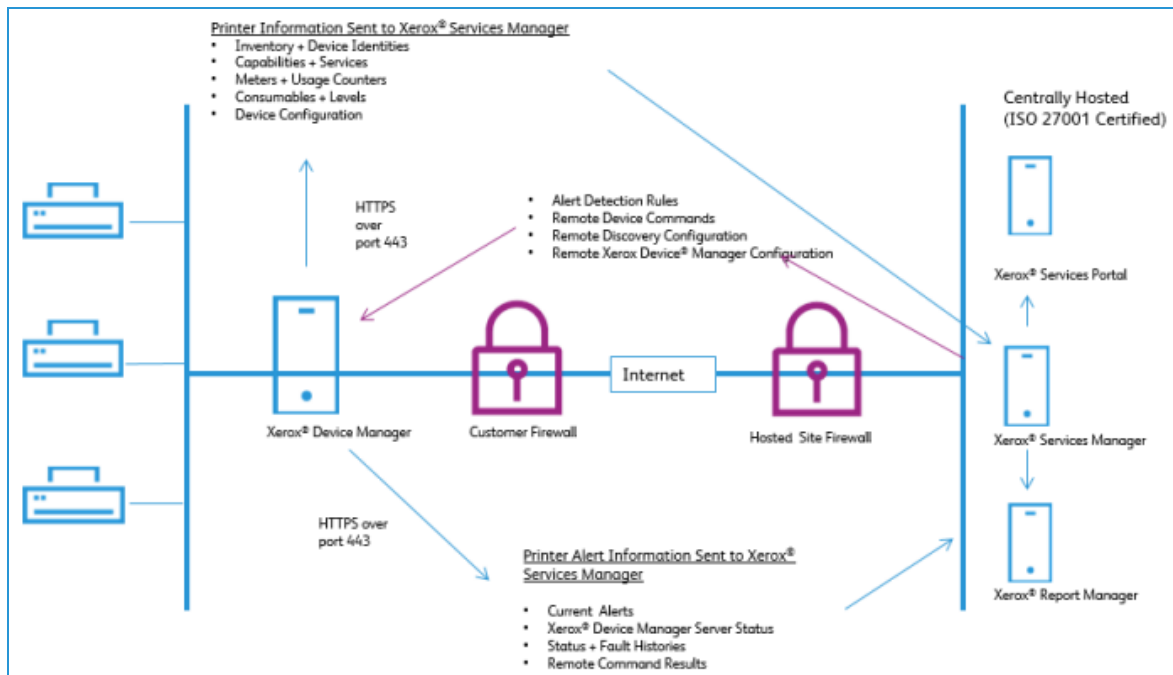
Machine Model	Job Data
Xerox® Nuvera® 144 CP	1.76 KB/job
Xerox® Nuvera® 144 EA	1.70 KB/job
Xerox® iGen	2.38 KB/job
Average	1.92 KB/job

Xerox® Device Manager Data Gathering Options

Note: When you want to pull data on any new jobs, you must you clear all the previous jobs first. Otherwise, Xerox® Device Manager will pull all the jobs from a device that it polled before and not import them.

Integrations with Xerox® Services Manager and the Hosted Deployment Model

When Xerox® Device Manager is used in conjunction Xerox® Services Manager, multiple Xerox® Device Manager servers can be employed to discover and monitor printers. The Xerox® Device Manager servers transfer the associated printer information to the Xerox® Services Manager module, which will store it in the SQL® server database and track the devices as assets. The asset information can then be mined and displayed through the use of the Xerox® Report Manager. As part of Xerox® Services Manager, you can use alerts to create and track incidents generated by the devices. In order to keep all of the elements within the suite informed, the applications transfer commands, data and status between them. The Hosted Services deployment model (similar to Figure 1) is shown again below for reference. The paragraphs following the diagram outline the types, sizes, and frequency of the information passed between the applications.



MPS (Hosted) Configuration

Xerox® Device Manager to Xerox® Services Manager Interactions

Xerox® Device Manager when configured to communicate with a Xerox® Services Manager server, does so through secure Web services (using HTTPS).

Note: The communication between Xerox® Device Manager and Xerox® Services Manager utilizes TLS 1.2 and AES-256 bit cipher suite. The public key certificate is RSA 2048 bit.

Web Services Security With MPS

The security of this communication method is protected by several mechanisms.

- The Xerox® Device Manager administrator must acquire both a valid Xerox® Services Manager URL and a valid Xerox® Services Manager account ID from the Xerox® Services Manager administrator.
- The Xerox® Device Manager administrator must then use Xerox® Device Manager to request registration with Xerox® Services Manager.
- The Xerox® Services Manager administrator must then accept the registration from Xerox® Device Manager.
- Xerox® Device Manager, when configured to communicate with a Xerox® Services Manager server, does so through secure Web services (using HTTPS).
- Xerox® Device Manager initiates all contact with Xerox® Services Manager.

Web Services Data Interactions With MPS

- The types of information that are exchanged between Xerox® Device Manager and Xerox® Services Manager include asset existence and identification, device usage, configuration, capabilities, customers, chargeback codes, job accounting data, policy log data, and remote commands. These numbers are for the data that is transmitted and do not include any extra data size created when sending the SOAP message.
- Xerox® Device Manager-specific configuration data pulls from the Auto Update Server, which, like Xerox® Services Manager, is also a secure Xerox MPS-hosted server. The configuration data includes firmware upgrade enablement, synthetic alert configuration, and protocol configuration set enablement.

Xerox® Device Manager registration is required to initialize or pair Xerox® Device Managers with Xerox® Services Manager for a given account:

- Data content includes account ID and Xerox® Device Manager ID.
- Data size is negligible (<2KB).
- Frequency is typically once when Xerox® Device Manager is first installed and then every time a new group or category needs to be mapped for alerts (very infrequent).

Once the Xerox® Device Manager site has been accepted, the export/import settings are created. You can schedule to have the data sent on a regular basis:

- Data content includes Xerox® Services Manager sweep settings, rediscovery settings, data export settings, SNMP community strings, SNMP timeout, and retries.
- Data size depends on the setting defined in the Xerox® Services Manager Sweep but will be ~2 KB at a minimum and can grow to be more than 9 KB.
- The import will occur every day at midnight without any user intervention.

Report Application Status occurs once the Xerox® Device Manager site has been accepted and can also be initiated from the Xerox® Services Manager page:

- Data content includes site information and server information including IP address, memory, hard drive size, and critical services.
- Data size is ~ 3 KB.
- Frequency is configurable and the default is every 60 minutes.

Export of printer information can be configured for both managed and unmanaged devices:

- Data content includes all fields that have been enabled for export and by default all data is exported.
 - Data size is ~35 KB per 100 devices.
 - Managed devices can be exported every hour, but unmanaged devices can only be exported every day.
- Note:** When Xerox® Device Manager is connected to hosted Xerox® Services Manager, export time is limited to every 6 hours.

Poll for Remote Commands: Periodically, Xerox® Device Manager will query Xerox® Services Manager if there are any remote commands to execute. Remote commands can be requests for status or reboot for example. When Remote Alerts are sent, they will come down as a Remote Command.

- Data content will be a No-Op if there are no commands to execute. If there is a command to execute, then the information about the Remote Command will be sent.
- Data size depends on the command and number of commands.
 - For a troubleshoot Device command the response will be 9 KB
 - If an Upgrade Device command is queued, Xerox® Device Manager will also retrieve the firmware file from the Xerox® Services Manager. Firmware files can be more than 100 MB.

Frequency is configurable and by default is set to five minutes.

Job Accounting Data: This data is reported by Xerox® Device Manager to Xerox® Services Manager, and can be configured for managed and unmanaged devices.

- Data content includes all fields that have been enabled for export, and by default only the selected fields are exported.
- Data size is ~1 KB per job.

Customers and Chargeback Codes: This data exchange depends on whether synchronization is enabled within Xerox® Device Manager. If synchronization is enabled, customer data will be periodically pulled down to Xerox® Device Manager from Xerox® Services Manager. Also, if Active Directory® or CSV file Customer Import is configured, Customer and chargeback code information will be periodically exported directly to Xerox® Services Manager through Xerox® Device Manager.

- For each customer, depending upon number of fields, Xerox® Services Manager upload data size can be on average ~1KB.
- For each customer, depending upon number of fields, Xerox® Services Manager download data size can be on average ~1KB.

Print Policy Log Data: This data exchange is from Xerox® Device Manager to Xerox® Services Manager. Policy logs are collected by Xerox® Device Manager for each policy violation against a print job document.

- For each policy log, the average data size is ~1KB.

Alternative Device Discover Methods

IP Easy Discovery

OPERATION

The IP Easy Discovery feature provides printer discovery with minimum user intervention. It consolidates the existing mechanisms of IP Subnet Scan, described below, and IP Sweep, described above, into a single, easy-to-use process. With this method, device discovery will be driven by the subnet information stored in the customer's network routers.

WHEN TO USE

The IP Easy Discovery method is a useful way to discover IP subnets on a network if you do not have first-hand knowledge of the company's IP subnet infrastructure.

NETWORK IMPACT

Before running this discovery, it may be necessary to exclude sensitive addresses from the discovery process. This is particularly important when scanning all subnets within a firewall.

ACCURACY

The IP Easy Discovery method is particularly useful in those environments that are open in terms of unrestricted subnets and whose routers have been enabled to pass SNMP queries. As the amount of network restrictions is increased, the less effective this approach tends to be.

IP Broadcast

OPERATION

A single packet is broadcast to every subnet defined within discovery's subnet list specification. Specifically:

- In this packet, Xerox® Device Manager requests a value for a single SNMP-based RFC 1213.
- For each device that responds to the RFC 1213 MIB OID, Xerox® Device Manager will add the IP address of the response packet into its list of live IP addresses.
- Xerox® Device Manager then queries those devices with live IP addresses for two more OIDs; one from RFC 1213 and one from RFC 1759. This enables Xerox® Device Manager to identify printing devices from non-printing devices. Both groups of devices are stored within the Xerox® Device Manager database; however, only printing devices are exposed via the Xerox® Device Manager UI.
- For those printer devices that respond to the RFC 1759 OID query, Xerox® Device Manager flags them as printers.
- For those devices that do not respond to the RFC 1759 OID query, Xerox® Device Manager then checks a RFC 1213 OID value against two registry key values to determine if the device is in fact a known printer. This is necessary because some printing devices (e.g., printers using external print server boxes, older printers, etc.) do not support RFC 1759 – the Printer MIB.
- The registry keys contain RFC 1213 values for several known supported and unsupported printers.

- Xerox® Device Manager then queries all live IP addresses for four additional OIDs; three RFC 1213 OIDs and one RFC 1514 / 2790 OID.
- For those devices identified as printers, Xerox® Device Manager queries three more RFC 1514/2790 OID and four more RFC 1759 OIDs to obtain some basic attributes of the printer.
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID and a new OID from the Internet Draft of the Printer MIB in order to obtain the printer's serial number.
- Xerox® Device Manager then queries three RFC 1759 OIDs in order to display the printing device's rated speed in pages per minute units (PPM).
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID(s) to obtain the printing device's software/firmware level.

WHEN TO USE

The IP Broadcast Discovery method can be used as a quick and easy method of populating the Xerox® Device Manager database. In order to populate the Xerox® Device Manager database with an initial set of printers, Xerox® Device Manager performs this broadcast on its local subnet the first time the application is started after installation.

NETWORK IMPACT

A sharp spike in network traffic usually occurs when these devices respond all at once—creating packet collisions.

ACCURACY

This discovery method is considered to be a less reliable way of discovering printers because packet collisions are likely to occur when all of the devices on a subnet respond to the single broadcast simultaneously. As a result of these collisions, some data may be lost from those printing devices attempting to respond to the initial broadcast packet.

IP ARP Cache Discovery

OPERATION

A table, usually called the ARP Cache, is implemented on all network routers and maintains a mapping between all of the devices (in its subnet) physical addresses (MAC) and assigned IP addresses. The ARP Cache Table is exposed via SNMP; therefore, Xerox® Device Manager can query it to find live addresses that can subsequently be queried to find printers.

Specifically:

- An SNMP-based broadcast packet is sent out to the local subnet. In this packet, Xerox® Device Manager requests a single RFC 1213 OID that it uses to identify routers from the list of responses received.
- Devices that do not have an SNMP agent currently running will not respond to this SNMP-based broadcast packet.
- It is important to note that the SNMP-based broadcast packet is only sent to the local subnet. Beyond the local subnet (hop count >0), only direct SNMP queries are made to known IP addresses.
- Xerox® Device Manager will then create two lists based upon all responses received on the local subnet:
- A list of live, non-router-related IP addresses
- A list of devices identified as routers

- If the hop count within the ARP Cache configuration page was set to 0, the address generation portion of discovery would stop at this point and Xerox® Device Manager would then begin to query each IP address for printer information.
- If the hop count within the ARP Cache configuration page is greater than 0 for those devices identified as routers, Xerox® Device Manager performs an SNMP Get-Table operation on each router's MIB version of the ARP Cache. This is done to build the list of live IP addresses that exist beyond the local subnet.
- For each IP address retrieved from a router's MIB-based ARP Cache, Xerox® Device Manager then performs the same SNMP query for an RFC 1213 OID. Again, Xerox® Device Manager is looking for those IP addresses that represent router devices. Similar algorithms apply as before:
- Those devices that do not have an SNMP agent currently running will not respond to this SNMP OID query. Therefore, Xerox® Device Manager will remove the IP addresses of such devices from the list of live IP addresses.
- The IP addresses for non-router-related devices that respond to the SNMP OID query will then be flagged with an appropriate hop count.
- The process of querying routers and MIB-based ARP Cache entries to identify live IP addresses continues until either the user-defined number of hops has been reached or when the MIB-based ARP Cache queries no longer yield new IP addresses. At this point, the address generation portion of the SNMP-based ARP Cache discovery operation is complete.
- The printer-related data gathering process begins in parallel with the live IP address gathering process once the list of live IP addresses begins to accumulate addresses.
- A single packet is sent to each live IP address discovered during the SNMP-based ARP Cache queries. In this packet, Xerox® Device Manager requests a value for a single SNMP-based RFC 1213 OID.
- For each device that responds to the RFC 1213 OID query, Xerox® Device Manager will save the value returned as the device's MAC address.
- Xerox® Device Manager then queries those devices with live IP addresses for two more OIDs; one from RFC 1213 and one from RFC 1759. This enables Xerox® Device Manager to identify printing devices from non-printing devices. Both groups of devices are stored within the Xerox® Device Manager database; however, only printing devices are exposed via the Xerox® Device Manager UI.
- For those printer devices that respond to the RFC 1759 query, Xerox® Device Manager flags them as printers.
- For those devices that do not respond to the RFC 1759 OID query, Xerox® Device Manager then checks the RFC 1213 OID value against two registry key values to determine if the device is in fact a known printer. This is necessary because some printing devices (e.g., printers using external print server boxes, older printers, etc.) do not support RFC 1759 – the Printer MIB.
- The registry keys contain a comma separated list of RFC 1213 OID values for several known supported and unsupported printers.
- Xerox® Device Manager then queries all live IP addresses for three RFC 1213 OIDs and one RFC 1514/2790 OID.
- For those devices identified as printers, Xerox® Device Manager queries three more RFC 1514/2790 OIDs and four more RFC 1759 OIDs to obtain some basic attributes of the printer.
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID and a new OID from the Internet Draft of the Printer MIB in order to obtain the printer's serial number.
- Xerox® Device Manager then queries three RFC 1759 OIDs in order to display the printing device's rated speed in pages per minute units.
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID(s) to obtain the printing device's software/firmware level.

WHEN TO USE

Like the IP Broadcast, it is a good method for obtaining a quick collection of printers on a network. For the ARP Cache discovery method to be effective, it should be run during business hours in order to increase the success rate for finding live IP addresses.

NETWORK IMPACT

The amount of traffic generated by the SNMP-based ARP Cache discovery is less than a Sweep discovery because the requests are directed to only live, known IP addresses instead of every possible address within the subnet/address range. Typically, the impact to the network is barely noticeable although a steady stream of packets can be seen. Also, router usage-related logs may grow in size due to this discovery method.

ACCURACY

Because it is based on dynamic router information, the ARP Cache discovery method is not as reliable as the SNMP Sweep method and must be used more frequently than the IP Sweep.

IP Sweep

OPERATION

SNMP Sweep Discovery sends a packet to every IP address in the user-defined subnet or address range list to generate a comprehensive list of devices responding at the endpoints.

Note: Routers can block or disable the ability to answer SNMP requests on some printers. When discovering computers, you can select whether or not to use WMI queries through RPC communication to computers that do not respond to ICMP pings. If not enabled (set by default), those computers that do not respond to an ICMP ping are considered “disconnected” and the discovery method moves on. Routers can block the ability to answer ICMP Ping requests or disabled at the computer. By adding the WMI interface to the Discovery method, more computers are found, but at the possible cost of additional network traffic due to the WMI RPC calls

WHEN TO USE

The SNMP Sweep Discovery method (IP Sweep) is the preferred method of accurately discovering printers on a network. It should be run during business hours in order to increase the success rate for finding live IP addresses.

NETWORK IMPACT

The amount of network traffic generated by a sweep-based discovery is minimized because the requests are directed to specific IP addresses defined by the user. Specific blocks can be included or excluded to reduce network traffic. With IP Sweep Discovery, you can add the Internet Printing Protocol (IPP) as a last resort during device querying, in the event that the device fails to respond to SNMP v1/v2 queries. By selecting this option, the Discovery process may experience significant delay in completing the sweep operation, and could introduce additional network traffic.

ACCURACY

The SNMP Sweep Discovery method (IP Sweep) offers results in a more controlled and orderly flow of data between printers and Xerox® Device Manager (unlike the Broadcast method).

SNMP V3 IP Sweep**OPERATION**

The SNMP V3 Discovery method allows multiple SNMP V3 devices to be discovered at one time. You can set up a discovery method and import a csv file of device addresses, subnets, or ranges with the V3 credentials. You can schedule device discovery so that new devices added to the network with the same credentials are automatically added to Xerox® Device Manager. SNMP V3 is the most secure; it uses authentication and encryption to provide enhanced security over what is supplied by SNMP V1/V2.

WHEN TO USE

Run SNMP V3 IP Sweep during business hours in order to increase the success rate for finding live IP addresses.

NETWORK IMPACT

The amount of network traffic generated by a sweep-based discovery is minimized because the requests are directed to specific IP addresses defined by the user. Specific blocks can be included or excluded to reduce network traffic.

ACCURACY

The SNMP V3 Sweep:

- Is the most reliable method of finding devices
- IP Address ranges are swept using SNMP V3 only
- The SNMP V3 Discovery method allows multiple SNMP V3 devices to be discovered at one time.

Subnet Scan**OPERATION**

Although this discovery method does not find printers, IP Subnet Scan finds the subnets that are available for printer discovery. The IP subnets found during this discovery method are made available to the IP Broadcast and the IP Sweep discovery methods.

Specifically:

- The list of known subnets is cleared.
- An SNMP-based broadcast packet is initially sent out to the local subnet. In this packet, Xerox® Device Manager requests a single RFC 1213 OID which it uses to identify routers from the list of responses received.
 - Only those devices that have SNMP agents currently running will respond to this broadcast packet.

- It is important to note that the SNMP-based broadcast packet is only sent to the local subnet. Beyond the local subnet (hop count >0), only direct SNMP queries are made to known IP addresses.
- Xerox® Device Manager will then create two lists based upon all responses received on the local subnet:
 - A list of live, non-router-related IP addresses
 - A list of devices identified as routers
- If the hop count within the IP Subnet Scan configuration page was set to 0, the address generation portion of discovery would stop at this point.
- If the hop count within the IP Subnet Scan configuration page is greater than 0 for those devices identified as routers, Xerox® Device Manager will then perform an SNMP Get-Table operation on each router's MIB version of the ARP Cache. This is done to continue to populate the router list and the live IP address list.
- For each IP address retrieved from a router's MIB-based ARP Cache, the Xerox® Device Manager application then performs the same SNMP query for an RFC 1213 OID. Again, Xerox® Device Manager is looking for those IP addresses that represent router devices. The same algorithms apply as before with just one modification:
 - Those devices that do not have an SNMP agent currently running will not respond to this SNMP OID query. Therefore, Xerox® Device Manager will remove the IP addresses of such devices from the list of live IP addresses.
 - Xerox® Device Manager then determines whether the new IP address fits within the known list of subnets.
- If the IP address is from a known IP subnet, Xerox® Device Manager moves to the next IP address within the list of live IP addresses.
- If the IP address is not from one of the known IP subnets, Xerox® Device Manager will use that IP address to determine its subnet mask by performing an SNMP query to a single RFC 1213 OID. From this data, Xerox® Device Manager calculates the subnet address and then adds this new subnet to the list of known subnets.
- The process of querying routers and MIB-based ARP Cache entries to identify IP subnets continues until either the user-defined number of hops has been reached or when the MIB-based ARP Cache queries no longer yield new IP addresses. At this point, the IP Subnet Scan discovery operation is complete.

WHEN TO USE

The IP Subnet Scan discovery method is a useful way to discover subnets on a network if you don't have first-hand knowledge of the company's IP infrastructure. However, this scan technique can take a long time to complete due to its thoroughness.

NETWORK IMPACT

The amount of traffic generated by an IP subnet based discovery is less than the ARP cache discovery method described above.

ACCURACY

This discovery method is only as accurate as the ARP Cache maintained by network routers. Furthermore, the number of IP subnets that can be detected is dependent upon the SNMP community names used by routers that are configured within the Administration>Discovery>SNMPv1/v2 page. If a SNMP community name used by a network router is not known to Xerox® Device Manager, those subnets will not be detected by this discovery method.

IPX Network Scan Discovery

OPERATION

The IPX Network Discovery mechanism uses the Service Advertisement Protocol (SAP) to find NetWare® servers and IPX networks by querying routers for attached IPX subnets. This method is not used to find printers, but rather the NetWare® components (NetWare® servers and networks) that know where IPX networked printers are located. The results of this scan are returned and displayed on the IPX Servers and IPX Addresses Discovery configuration pages, making it easier to configure information for these methods (discussed below). The results also appear on the page in the servers and networks found in Last Scan section.

Specifically:

- An SAP broadcast packet is sent to the local sub-network. This packet is a type 4-based (servers only) SAP broadcast packet that is used to obtain a list of all available Novell® NetWare® servers connected to the local sub-network.
- Novell® NetWare® servers maintain a complete list of NetWare® servers and each server's corresponding internal IPX network number.
- Each Novell® NetWare® server connected to the local sub-network will respond to the SAP broadcast with its list of known NetWare® servers and corresponding internal IPX network numbers.
- Xerox® Device Manager then queries each internal IPX network number received for its corresponding external IPX network number using SNMP and a Novell®-unique OID
 - The external network number is used for display purposes only. Most print vendors' configuration pages display the external IPX network number that the printer is using instead of the internal IPX network number. Therefore, to ensure that the IPX address information obtained from a printer can be used by the Xerox® Device Manager application, the external IPX network number is displayed.
 - Xerox® Device Manager uses the IPX internal network number when communicating with servers and printers.
- The external IPX network number operation continues until all internal IPX network numbers have been queried.

The data obtained by this discovery method is made available to the IPX Servers and the IPX Addresses discovery methods discussed below.

WHEN TO USE

IPX Network Scan is useful when you do not know all of the IPX networks and server combinations at your site.

NETWORK IMPACT

The amount of traffic generated by an IPX network scan discovery is very light, and it is extremely quick when compared with other Xerox® Device Manager discovery methods. This is because only an initial SAP broadcast packet is transmitted over the network followed by an SNMP packet for each NetWare® server that responded to the SAP broadcast packet. However, it is the broadcast of SAP packets that creates a fair amount of network traffic, depending upon the number of Novell® NetWare® servers connected to the network and whether routers are configured to pass SAP broadcasts.

ACCURACY

This discovery method is very good at detecting NetWare® servers connected to the network. However, it is only marginally successful at detecting the corresponding IPX Network Address of those servers. IPX Network Scan provides accurate information, so that you do not have to know all of the IPX networks and server combinations at your site, which makes the configuration process more efficient and improves overall discovery results.

Notes:

- A Novell® server must be present on the local subnet or at least be reachable via SAP broadcast across a router; otherwise, Xerox® Device Manager will not be able to discover printers running the IPX protocol.
- If an account does not allow SAP Broadcast packets to traverse their routers, a complete list of Novell® NetWare® servers will be more difficult to obtain. In this case, knowledge of the network topology will be required. Use the IPX Server Discovery method discussed below and manually add the IPX server name in the servers for Printer Discovery>Specify NetWare® Server tile.
- If the network topology is known and there are a large number of NetWare® servers to import, an Xerox® Device Manager utility is provided to import those from a list file. Browse to C:\Program Files\Xerox\Xerox Device Manager\DBscripts for a program named DiscoDBui.
- Use dynamic groups to automatically identify printers running the IPX protocol
- Printers running the IPX protocol typically perform an SAP broadcast to announce its presence when connecting to a network segment. Any Novell® NetWare® server that is connected to the same network segment will detect this SAP broadcast and will update its SAP table accordingly. This SAP table is very similar in concept to the routers ARP Cache.
- The Xerox® Device Manager application's configurable timeout value will impact the performance of IPX-based communications. (e.g., IPX SAP, IPX NCP, IPX SNMP, etc.) Therefore, only adjust this value if known IPX-based printers do not appear within the Xerox® Device Manager database.

IPX Server Discovery**OPERATION**

As described above, NetWare® uses the Service Advertising Protocol (SAP) which allows file servers, print servers and application servers to advertise their services and addresses. Xerox® Device Manager broadcasts an SAP packet across the network and these servers respond with the information about them.

Specifically, Xerox® Device Manager:

- Creates a NetWare® Core Protocol (NCP) connection with the Novell® NetWare® Server in order to establish communication.
- Queries the Novell® NetWare® server's SAP tables for printers with a particular SAP type ID. This ID is unique to each printer vendor (e.g. Xerox = 1900h, Tektronix = 0535h, etc.)
- The Novell® NetWare® Server will then respond with a single device whose SAP type ID matches the requested Xerox® Device Manager printer ID. The data contained within this response includes the printer's IPX network number and node address.
- The device's address is added to the list of live IPX device addresses.
- Xerox® Device Manager then sends another NCP request to the Novell® NetWare® server to get the next device whose SAP type ID matches the requested Xerox® Device Manager printer ID. The Novell® NetWare® server's response is processed as described previously.
- This request/response process continues until all devices for each SAP ID have been retrieved. This scan operation is very similar in concept to an SNMP Get-Next operation performed on a printer. (i.e., An MIB

- browser continues to receive responses to the GET-NEXT PDU until an SNMP error is received indicating that the printer has reached the end of its supported MIB objects.)
- At this point, Xerox® Device Manager has a complete list of IPX-based printers that are communicating with the current Novell® NetWare® server

WHEN TO USE

Use this method after performing an IPX Network Scan to determine Novell® server address information.

NETWORK IMPACT

We expect minimal impacts to the because direct queries are restricted to known servers.

ACCURACY

IPX server-based discovery is the quicker and more accurate of the two IPX discovery methods provided by Xerox® Device Manager (IPX Server and IPX address).

IPX Address Scan Discovery

OPERATION

This discovery method will query the IPX addresses returned from the IPX Network Scan and Server Discovery for print devices.

Specifically:

- A single packet is sent to each IPX address selected within the IPX Addresses configuration page. In this packet, Xerox® Device Manager requests a value for a single SNMP-based RFC 1213 OID.
- For each device that responds to the RFC 1213 OID, Xerox® Device Manager will add the IPX address of the response packet into its list of live IPX addresses.
- Xerox® Device Manager then queries those devices with live IPX addresses for two more OIDs; one RFC 1213 OID and one RFC 1759 OID. This enables Xerox® Device Manager to identify printing devices from non-printing devices. Both groups of devices are stored within the Xerox® Device Manager database, however, only printing devices are exposed via the Xerox® Device Manager UI.
 - For those printer devices that respond to the RFC 1759 OID query, Xerox® Device Manager flags them as printers.
 - For those devices that do not respond to the RFC 1759 OID query, Xerox® Device Manager then checks the RFC 1213 OID value against two registry key values to determine if the device is in fact a known printer. This is necessary because some printing devices (e.g., printers using external print server boxes, older printers, etc.) do not support RFC 1759 – the Printer MIB.
- The registry keys contain a comma separated list of RFC 1213 values for several known supported and unsupported printers.
- Xerox® Device Manager then queries all live IPX addresses for three RFC 1213 OIDs and one RFC 1514/2790 OID.
- For those devices identified as printers, Xerox® Device Manager queries three more RFC 1514/2790 OIDs and four more 1759 to obtain some basic attributes of the printer.
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID and a new OID from the Internet Draft of the Printer MIB in order to obtain the printer's serial number.

- Xerox® Device Manager then queries three RFC 1759 OIDs in order to display the printing device's rated speed in pages per minute units.
- Based upon the identity of each printing device, Xerox® Device Manager then queries the appropriate vendor-specific OID(s) to obtain the printing device's software/firmware level.

WHEN TO USE

Use this method after performing an IPX Network Scan and IPX server discovery to determine print device information connected to those addresses.

NETWORK IMPACT

We expect minimal impacts to the network because direct queries are restricted to known addresses.

ACCURACY

This method may return less IPX-based printers than will be returned by an IPX Server discovery method.

Note: The Xerox® Device Manager application's configurable timeout value will impact the performance of IPX-based communications. Therefore, only adjust this value if known IPX-based printers do not appear within the Xerox® Device Manager database.

Summary and Next Steps

By this point, the user should have answers to the following FAQs that were indicated in Section 1:

What additional hardware and software will be introduced to my IT world?

- The team will install the Wintel server-class systems with Xerox developed software depending on the operability model (hosted or on-site), locations, and network configurations of the devices to be managed and the Xerox® Device Manager options.
- Optionally, a thin-client job tracking application will be installed on print servers and workstations.

What typical loads and bandwidth demands will be made on my network?

- Sample calculations have been provided; actual demands will be based on amount and frequency of use.

What new user accounts will be created and what existing accounts (if any) will be touched by this application?

- A CentreWare® user account may be created with local administrative privileges, and depending on any requirement to manage remote devices and queues, it may need to accept domain-based administration privileges.
- An existing administrator account could be substituted for the default (Run As).

What network protocols and IP ports will be used by this application?

- Tables of information are provided; the actual protocols and ports that are used depend on the operability model and options required.

What levels of network and e-mail security are incorporated within/around Xerox® Device Manager?

- User Authentication and Authorization, group policy administration, and data encryption
- TCP port monitoring and restriction
- Standard SMTP e-mail security capabilities
- SNMP community string naming

What will the impact to my printing environment be after this application is installed?

- The printers under management will create and consume SNMP-based traffic on the network within some predefined time windows.
- The printers will be reporting status, failures, job activities, and usage information to a central location (Xerox® Device Manager).
- Printer driver downloading may be performed remotely.

What other impacts/effects will exist (i.e. to people, processes, or products)?

- Normal server maintenance and floor space will be required on the MPS servers located behind the client's firewall. Consideration on who will perform the periodic backup of the two Xerox® Device Manager SQL Server® databases and the hopefully little-needed database restore.

Appendix

Firmware Upgrade Information

- Firmware Upgrades are handled via Firmware Upgrade Policies. Policies can be created to apply to an entire fleet, groups of devices, or to a single device.
- Firmware Upgrade supports up to 500 firmware upgrades at one time.
- Retries can be scheduled and failed updates can be restarted.
- Upgrade files are sent to one device at a time.
 - Verification of the upgrade is done after all firmware files have been sent.
- The Fleet Orchestrator feature distributes the network load when deploying to Xerox® Altalink® devices. Xerox® Device Manager can select devices automatically within the same subnet to act as distribution hubs for the firmware files. This reduces the overall time it takes to upgrade a fleet of devices.

Internet Information Server 7(IIS7) Internet Information Server (IIS) can limit the Firmware Upgrade file size Xerox® Device Manager can upload. The following command is an example of how to change the supported maximum content allowed by IIS to allow for larger firmware files:

```
%windir%\system32\inetsrv\appcmd set config "Default Web Site/XeroxDeviceManager" -  
section:requestFiltering -requestLimits.maxAllowedContentLength:524288000
```

Note that the maxAllowedContentLength has been set to the maximum Firmware file Xerox® Device Manager supports of 500MB.

The maxAllowedContentLength should also be modified with IIS by downloading the IIS Admin Pack and then following the steps on the below website:

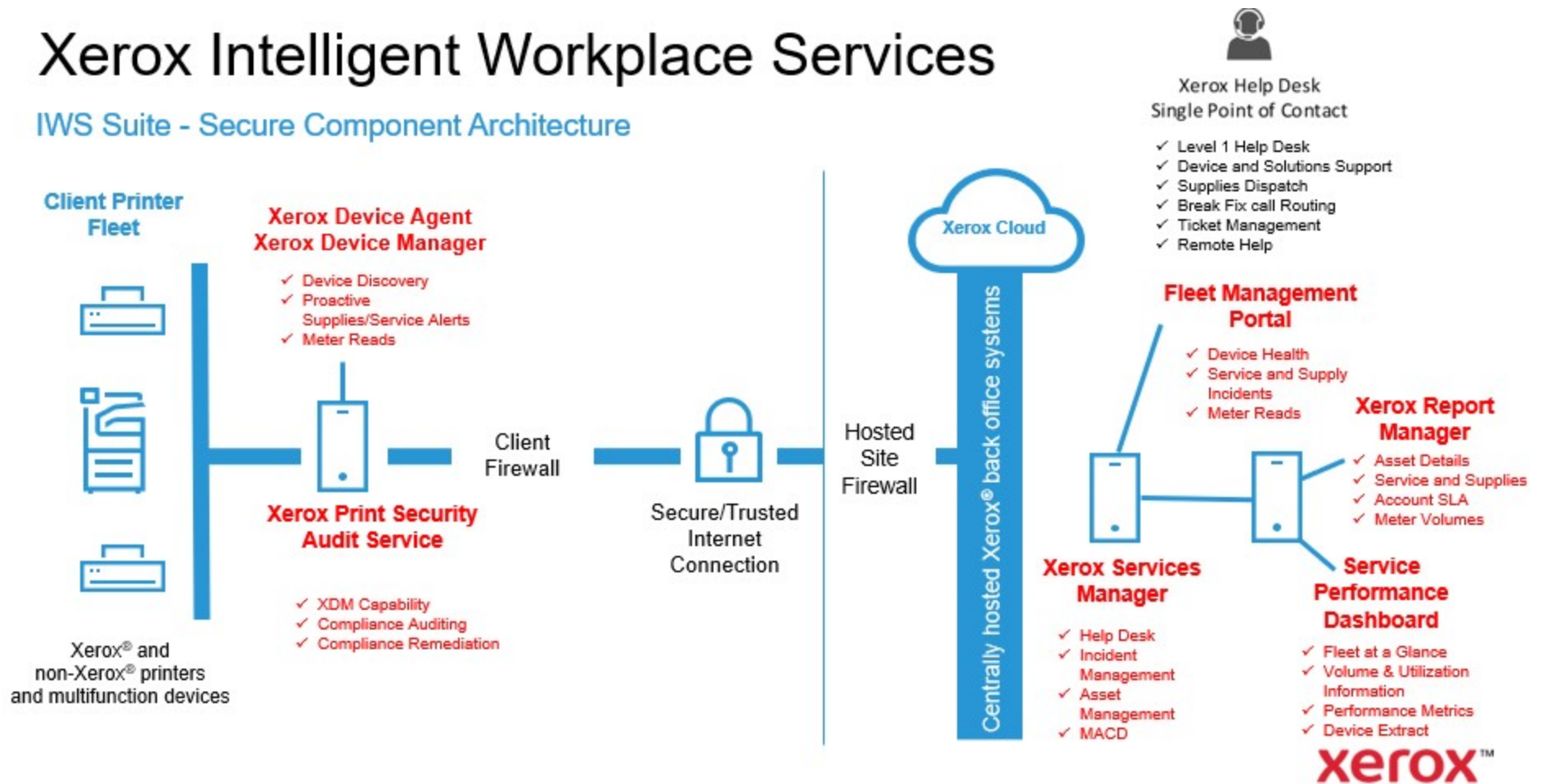
Admin Pack Download: <http://www.iis.net/download/AdministrationPack>

Refer to the website below to modify IIS Request Filtering.

<http://www.iis.net/ConfigReference/system.webServer/security/requestFiltering>

Xerox Intelligent Workplace Services

IWS Suite - Secure Component Architecture



Security Guide

Xerox® VersaLink® B405/B605/B615/B7025/B7030/B7035,
C405/C505/C605/C7020/C7025/C7030 Multifunction Products

Xerox® VersaLink® B400/B600/B610,
C400/C500/C600/C7000/C8000/C9000 Printers



© 2019 Xerox Corporation. All rights reserved. Xerox®, CentreWare®, FreeFlow®, PrimeLink®, Xerox Extensible Interface Platform® are trademarks of Xerox Corporation in the United States and/or other countries. BR27410

Other company trademarks are also acknowledged.

Document Version: 1.1 (January 2020).

Copyright protection claimed includes all forms and matters of copyrightable material and information now allowed by statutory or judicial law or hereinafter granted including without limitation, material generated from the software programs which are displayed on the screen, such as icons, screen displays, looks, etc.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

Table of Contents

1. Introduction	vi
Purpose	vi
Target Audience	vi
Disclaimer	vi
2. Product Description	3-1
Physical Components	3-1
Architecture	3-2
User Interface	3-2
Scanner	3-2
Marking Engine	3-2
Controller	3-3
Controller External Interfaces	3-3
Front Panel USB (Type A) port(s)	3-3
10/100/1000 MB Ethernet RJ-45 Network Connector	3-3
Rear USB (Type B) Target Port	3-3
Optional Equipment.....	3-4
RJ-11 Analog Fax and Telephone	3-4
Wireless Network Connector.....	3-4
Near Field Communications (NFC) Reader	3-4
SMART CARD – CAC/PIV	3-4
Foreign Product Interface.....	3-4
3. User Data Protection.....	4-1
User Data Protection While Within Product	4-1
Encryption	4-1
Trusted Platform Module (TPM Chip)	4-1
Media Sanitization (Image Overwrite)	4-1
Overwriting Immediate Image Overwrite.....	4-2
On-Demand Image Overwrite	4-2
User Data in Transit	4-2
Inbound User Data (Print Job Submission).....	4-2
Scanning to Network Repository, Email, Fax Server (Outbound User Data)	4-3

Scanning to User Local USB Storage Product (Outbound User Data).....	4-3
Add on Apps – Cloud, Google, DropBox, and others (Outbound User Data).....	4-4
4. Network Security	5-1
TCP/IP Ports and Services	5-1
Listening Services (inbound ports).....	5-2
Network Encryption	5-3
IPSec.....	5-3
Wireless 802.11 Wi-Fi Protected Access (WPA)	5-3
TLS.....	5-4
Public Key Encryption (PKI)	5-4
Device Certificates	5-5
Trusted Certificates	5-6
Certificate Validation	5-6
Email Signing and Encryption using S/MIME.....	5-7
SNMPv3	5-7
Network Access Control.....	5-8
802.1x.....	5-8
Cisco Identity Services Engine (ISE)	5-8
Contextual Endpoint Connection Management	5-9
FIPS140-2 Compliance Validation	5-9
Additional Network Security Controls.....	5-10
Endpoint Firewall Options	5-10
IP Whitelisting (IP Address Filtering)	5-10
Stateful Firewall (Advanced IP Filtering).....	5-10
Personal Identifiable Information (PII).....	5-10
5. Device Security: BIOS, Firmware, OS, Runtime, and Operational Security Controls	6-1
Pre-Boot BIOS Protection	6-1
BIOS.....	6-1
Embedded Encryption.....	6-1
Boot Process Integrity	6-1
Firmware Integrity & Verification	6-1
Event Monitoring & Logging	6-1
Event Monitoring and Logging	6-1
Continuous Operational Security	6-1

Firmware and Diagnostic Security Controls	6-1
Fail Secure Vs Fail Safe.....	6-2
Pre-Boot Security	6-2
BIOS	6-2
Embedded Encryption	6-2
Boot Process Security	6-2
Firmware Integrity	6-2
Runtime Security	6-1
Event Monitoring and Logging	6-4
Audit Log	6-4
Operational Security.....	6-4
Firmware Restrictions	6-4
Service Technician (CSE) Access Restriction	6-5
Additional Service Details	6-5
Backup and Restore (Cloning)	6-5
EIP Applications	6-5
XCP (eXtensible Customizable Platform)	6-6
6. Configuration and Security Policy Management Solutions	7-1
7. Identification, Authentication, and Authorization	8-1
Authentication	8-1
Local Authentication	8-1
Password Policy	8-2
Network Authentication	8-2
Smart Card Authentication	8-2
Convenience Authentication	8-3
Simple Authentication (non-secure).....	8-3
Authorization (Role Based Access Controls)	8-3
Remote Access	8-3
Local Access	8-3
8. Additional Information and Resources	9-1
Security @ Xerox®	9-1
Responses to Known Vulnerabilities.....	9-1
Additional Resources	9-1
9. Appendix A: Product Security Profiles	10-2

VersaLink B7025/B7030/B7035	10-2
Physical Overview	10-2
Security Related Interfaces	10-3
Encryption and Overwrite	10-3
Controller Non-Volatile Storage	10-3
Controller Volatile Memory	10-4
Marking Engine Non-Volatile Storage	10-4
Marking Engine Volatile Memory	10-4
VersaLink C7000/C7020/C7025/C7030.....	10-5
Physical Overview	10-5
Security Related Interfaces	10-6
Encryption and Overwrite	10-6
Controller Non-Volatile Storage	10-6
Controller Volatile Memory	10-7
Marking Engine Non-Volatile Storage	10-7
Marking Engine Volatile Memory	10-7
VersaLink B400/B405	10-8
Physical Overview	10-8
Security Related Interfaces	10-9
Encryption and Overwrite	10-9
Controller Non-Volatile Storage	10-9
Controller Volatile Memory	10-10
Marking Engine Non-Volatile Storage	10-10
Marking Engine Volatile Memory	10-10
VersaLink C400/C405	10-11
Physical Overview	10-11
Security Related Interfaces	10-12
Encryption and Overwrite	10-12
Controller Non-Volatile Storage	10-12
Controller Volatile Memory	10-13
Marking Engine Non-Volatile Storage	10-13
Marking Engine Volatile Memory	10-13
VersaLink C500/C600/C505/C605.....	10-14
Physical Overview	10-14
Security Related Interfaces	10-15

Encryption and Overwrite	10-15
Controller Non-Volatile Storage	10-15
Controller Volatile Memory	10-16
Marking Engine Non-Volatile Storage	10-16
Marking Engine Volatile Memory	10-16
VersaLink B600/B605/B610/B615	10-17
Physical Overview	10-17
Security Related Interfaces	10-18
Encryption and Overwrite	10-18
Controller Non-Volatile Storage	10-18
Controller Volatile Memory	10-19
Marking Engine Non-Volatile Storage	10-19
Marking Engine Volatile Memory	10-19
VersaLink C8000/C9000	10-20
Physical Overview	10-20
Security Related Interfaces	10-21
Encryption and Overwrite	10-21
Controller Non-Volatile Storage	10-21
Controller Volatile Memory	10-22
Marking Engine Non-Volatile Storage	10-22
Marking Engine Volatile Memory	10-22
10. Appendix B: Security Events	11-1
Xerox VersaLink Security Events	11-1

1.

2. Introduction

Purpose

The purpose of this document is to disclose information for the VersaLink® multifunction devices and printers (hereinafter called as “the product” or “the system”) with respect to product security. Product Security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a network environment, and how the product may be accessed both locally and remotely. The purpose of this document is to inform Xerox customers of the design, functions, and features of the product with respect to Information Assurance. This document does not provide tutorial level information about security, connectivity, or the product’s features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

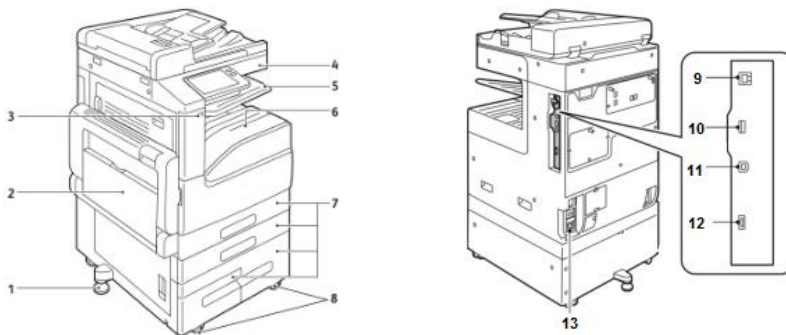
Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

3. Product Description

Physical Components

VersaLink® products consist of an input document handler and scanner, marking engine, controller, and user interface. A typical configuration is depicted below. Please note that options including finishers, paper trays, document handlers, etc. may vary configuration, however, they are not relevant to security and are not discussed.

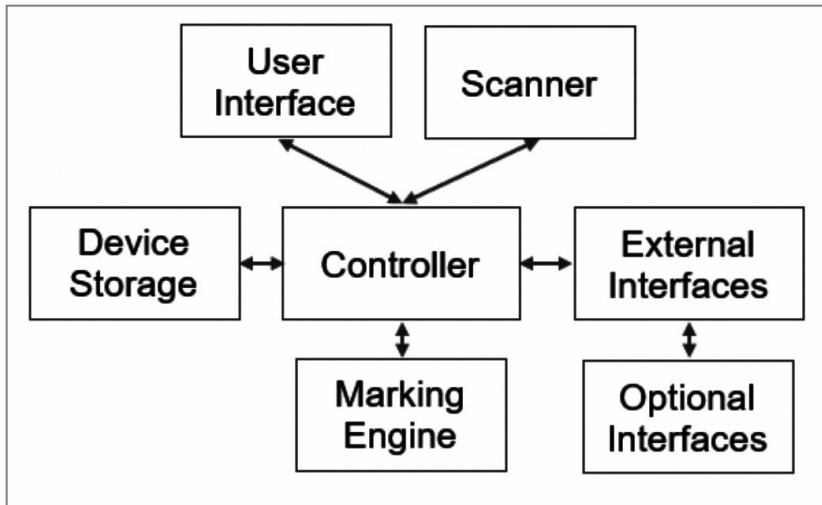


- | | |
|--|---|
| <ul style="list-style-type: none">1. Stabilizer.2. Bypass paper feed tray.3. Front USB Port(s)*4. Touch screen user interface.5. Upper paper tray.6. Lower paper tray.7. Paper feed trays. | <ul style="list-style-type: none">8. Caster wheels.9. Rear USB Port(s)*10. Optional Wi-Fi dongle port*11. RJ45 Ethernet connection*12. Service port
(May require disassembly to access).13. AC Power |
|--|---|

*Denotes a security related component

Architecture

VersaLink® products share a common architecture which is depicted below. The following sections describe components in detail.



User Interface

The user interface detects soft and hard button actuations and provides text and graphical prompts to the user. The user interface is sometimes referred to as the Graphical User Interface (GUI) or Local UI (LUI) to distinguish it from the remote web server interface (WebUI).

The user interface allows users to access product services and functions. Users with administrative privileges can manage the product configuration settings. User permissions are configurable through Role Based Access Control (RBAC) policies, described in section 7 Identification, Authentication, and Authorization

Scanner

The scanner converts documents from hardcopy to electronic data. A document handler moves originals into a position to be scanned. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images.

Marking Engine

The Marking Engine performs copy/print paper feeding and transport, image marking, fusing, and document finishing. The marking engine is comprised of paper supply trays and feeders, paper transport, LED scanner, xerographics, and paper output and finishing. The marking engine is only accessible to the Controller via inter-chip communication with no other access and does not store user data.

Controller

The controller manages document processing using proprietary hardware and algorithms to process documents into high-quality electronic and/or printed reproductions. Documents may be temporarily buffered in RAM during processing. Some models may be equipped with additional storage options such as magnetic Hard Disk Drive (HDD), Solid State Disk (SSD), SD Card, or Flash media. For model specific details please see Appendix A: Product Security Profiles. VersaLink® products encrypt user data and include media sanitization (overwrite) options that ensure that erased data cannot be recovered, described further in section 3 User Data Protection.

In addition to managing document processing the controller manages all network functions and services. Details can be found in section Network Security.

The controller handles all I/O communications with connected products. The following section provides a description of each interface. Please note that not all interfaces are supported on all models; details about each model can be found in Appendix A: Product Security Profiles.

Controller External Interfaces

Front Panel USB (Type A) port(s)

One or more USB ports may be located on the front of the product, near the user interface. Front USB ports may be enabled or disabled by a system administrator. The front USB port supports the following:

- Walk-up users may insert a USB thumb drive to store or retrieve documents for scanning and/or printing from a FAT formatted USB device. The controller will only allow reading/writing of a limited set of known document types (such as DOC, PDF, PNG, JPEG, TIFF, etc.). Other file types including binary executables are not supported.

Note: Features that use the front USB ports (such as Scan To USB) can be disabled independently or restricted using role-based access controls.

- Connection of optional equipment such as NFC or CAC readers.
- Firmware updates may be submitted through the front USB ports. (Note that the product must be configured to allow local firmware updates, or the update will not be processed.)

10/100/1000 MB Ethernet RJ-45 Network Connector

This is a standard RJ45 Ethernet network connector and conforms to IEEE Ethernet 802.3 standards.

Rear USB (Type B) Target Port

A USB type B port located on the controller board at the rear of the product. This port supports the following:

- USB target connector used for printing

Note: This port cannot be disabled completely by a system administrator.

Optional Equipment

RJ-11 Analog Fax and Telephone

The analog fax module connects to the controller. The fax connection supports the Fax Modem T.30 protocol only and will not accept data or voice communication attempts. An external (EXT) is available to connect an external handset. In this configuration, the FAX card acts as a passive relay.

Wireless Network Connector

VersaLink® products accept an optional wireless module via a proprietary port.

Near Field Communications (NFC) Reader

The system supports an installable RFID reader for authentication and convenience in certain configurations. VersaLink® products accept the RFID reader via USB on the front of the product. This communication cannot write or change any settings on the system. The data exchanged is not encrypted and may include information including system network status, IP address and product location. NFC functionality can be disabled using the embedded web server of the product. NFC functionality requires a software plugin that can be obtained from Xerox sales and support. NFC functionality is supported via optional touch screen user interface or optional dedicated NFC USB dongle.

Information shared over NFC includes: IPv4 Address, IPv6 Address, MAC Address, UUID (a unique identifier on the NFC client), and Fully qualified domain name

SMART CARD – CAC/PIV

All VersaLink® products support CAC/PIV login by enabling the VersaLink® Plug-in feature and then enabling the appropriate plug-in. Additional plug-ins can be downloaded from Xerox.com in the product Support area online.

All VersaLink® products support SIPR network access through a plug-in. The SIPR network plug-in is restricted only to users who have purchased the SIPR kit from Xerox. Contact your Xerox sales representative for details.

Foreign Product Interface

This port is used to connect optional equipment to control access to the machine. A typical application is a coin-operated product where a user must deposit money to enable the machine to print. The information available via the Foreign Product Interface is limited to optically-isolated pulses that can be used to count impressions marked on hardcopy sheets. No user data is transmitted to or from this interface.

4. User Data Protection

Xerox printers and multifunction products receive, process, and may optionally store user data from several sources including as local print, scan, fax, or copy jobs or mobile and cloud applications, etc. Xerox products protect user data being processed by employing strong encryption. When the data is no longer needed, the Image Overwrite (IIO) feature automatically erases and overwrites the data on magnetic media, rendering it unrecoverable. As an additional layer of protection, an extension of IIO called On-Demand Image Overwrite (ODIO) can be invoked to securely wipe all user data from magnetic media.

User Data Protection While Within Product

This section describes security controls that protect user data while it is resident within the product. For a description of security controls that protect data in transit please refer to the following section that discusses data in transit; also, the Network Security section of this document.

Encryption

All user data being processed or stored to the product is encrypted by default.

The algorithm used in the product is AES-256. The encryption key is automatically created at start up and stored in the RAM. The key is deleted by a power-off, due to the physical characteristics of the RAM.

Trusted Platform Module (TPM Chip)

Some models include a Trusted Platform Module (TPM). The TPM is compliant with ISO/IEC 11889, the international standard for a secure cryptoprocessor, dedicated to secure cryptographic keys. The TPM is used to securely hold the product storage encryption key. Please refer to Appendix A: Product Security Profiles for model specific information.

Media Sanitization (Image Overwrite)

VersaLink® products equipped with magnetic hard disk drives are compliant with NIST Special Publication 800-88 Rev1: Guidelines for Media Sanitization. User data is securely erased using a three-pass algorithm as described in the following link:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf>

Note: Solid-State storage media such as Solid-State Disk, eMMC, SD-Card, and Flash media cannot be completely sanitized by multi-pass overwriting methods due to the memory wear mapping that occurs. (Additionally, attempts to do so would also greatly erode the operational lifetime of solid-state media). Solid State media is therefore not recommended for use in highly secure environments. Please refer to NIST-800-88 “Table A-8: Flash Memory-Based Storage Product Sanitization” for technical details.

Overwriting Immediate Image Overwrite

When enabled, Immediate Image Overwrite (IIO) will overwrite any temporary files that were created on the magnetic hard disk that may contain user data. The feature provides continuous automatic of sensitive data with minimal impact to performance, robust error reporting, and logging via the Audit Log.

On-Demand Image Overwrite

Complementing the Immediate Image Overwrite is On-Demand Overwrite (ODIO). While IIO overwrites individual files, ODIO overwrites entire partitions. The ODIO feature can be invoked at any time and optionally may be scheduled to run automatically.

User Data in Transit

This section focuses on the protection of user data (print/scan/other jobs) in transit as they are submitted to the product for processing and/or are sent from the product to other systems. Additional protections are also discussed in the Network Security section of this document.

Inbound User Data (Print Job Submission)

In addition to supporting network level encryption including IPsec and WPA Xerox products also support encryption of print job data at the time of submission. This can be used to securely transmit print jobs over unencrypted connections or to enhance existing network level security controls.

Encrypted Transport	Description
IPPS (TLS)	Submit print jobs via Secure Internet Printing Protocol. This protocol is based on HTTP and utilizes the TLS suite to encrypt data.
HTTPS (TLS)	Securely submit a print job directly to product via the built-in web server.
Xerox Print Stream Encryption	The Xerox Global Print Driver® supports document encryption when submitting Secure Print jobs to enabled products. Simply check the box to Enable Encryption when adding the Passcode to the print job.

Scanning to Network Repository, Email, Fax Server (Outbound User Data)

VersaLink® multifunction products support scanning of hardcopy documents to external network locations including file repositories and email and facsimile services. In addition to supporting network level encryption including IPsec Xerox products support the following.

Protocol	Encryption	Description
HTTP	N/A	Unencrypted HTTP protocol.
HTTPS (TLS)	TLS	HTTP encrypted by TLS
FTP	N/A	Unencrypted FTP.
SFTP (SSH)	SSH	FTP encrypted by SSH through “EIP” ONLY
SMBv3	N/A	Encryption may be enabled on a Windows share. VersaLink® products do not currently support SMB encryption.
SMBv2	N/A	Unencrypted SMB
SMBv1	N/A	(Not used as a transport protocol. Used for network discovery only)
SMTP (email)	S/MIME	The product uses SMTP to transmit data to the email server. Email authentication, encryption, and signing are supported. Please refer to the Network Security section of this document for details.

Scanning to User Local USB Storage Product (Outbound User Data)

Scan data is transferred directly to the user’s USB product. Filesystem encryption of user products are not supported.

Add on Apps – Cloud, Google, DropBox, and others (Outbound User Data)

The Xerox App Gallery® contains several additional applications that extend the capabilities of Xerox products. Discussion of App security is beyond the scope of this document. Xerox Apps utilize the security framework provided by the third-party vendor. (For example, Microsoft O365 or Google apps would utilize Microsoft and Google's security mechanisms respectively). Please consult documentation for individual Apps and third-party security for details.

	VersaLink® Multifunction	VersaLink® Printers
	B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Local Data Encryption (HDD, SDD, IC, SD Card)	AES-256	AES-256
Federal Information Protection Standard 140-2	Yes	Yes
Media Sanitization NIST 800-171 (Image Overwrite)	Models with magnetic HDD. See Appendix A: Product Security Profiles	Models with magnetic HDD. See Appendix A: Product Security Profiles
Print Submission		
	IPPS (TLS)	Supported
	HTTPS (TLS)	Supported
	Xerox Print Stream Encryption	(Not currently supported)
Scan to Repository Server		
	HTTPS (TLS)	(Not currently supported)
	SFTP (SSH)	(Not currently supported)
	SMB (unencrypted)	v3
	SMB (with share encryption enabled)	(Not currently supported)
	HTTP (unencrypted)	(Not currently supported)
	FTP (unencrypted)	(Not currently supported)
Scan to Fax Server		
	HTTPS (TLS)	(Not currently supported)
	SFTP (SSH)	(Not currently supported)
	SMB (unencrypted)	v3
	SMB (with share encryption enabled)	(Not currently supported)
	S/MIME	Supported
	HTTP (unencrypted)	(Not currently supported)
	FTP (unencrypted)	(Not currently supported)
	SMTP (unencrypted)	Supported
Scan to Email		
	S/MIME	Supported
	SMTP (unencrypted)	Supported

5. Network Security

Xerox products are designed to offer a high degree of security and flexibility in almost any network environment. This section describes several aspects of the product related to network security.

TCP/IP Ports and Services

Xerox devices are robust, offering support for a wide array of services and protocols. The devices are capable of hosting services as well as acting as a client for others. The diagram below presents a high-level overview of inbound communications (from other hosts on the network into listening services on the device) and outbound connections initiated by the device (acting as a client to external network services).



Listening Services (inbound ports)

The following table summarizes all potentially open ports on the product. These ports can be enabled/disabled within the product configuration.

Port	Type	Service Name
80 or 443	TCP	HTTP including: Web User Interface UPnP Discovery Web Services for Products (WSD) WebDAV
631 or 443	TCP	HTTP (IPP)
137	UDP	NETBIOS (Name Service)
138	UDP	NETBIOS (Datagram Service)
161	UDP	SNMP
427	TCP/UDP	SLP
445	TCP	CIFS
500 & 4500	UDP	IPSec
515	TCP	LPR
631	TCP	IPP
1900	UDP	SSDP
3702	TCP	WSD (Discovery)
5353	UDP	mDNS
9100	TCP	Raw IP (also known as JetDirect, AppSocket or PDL-datastream)
5909-5999	TCP	Remote Access to local display panel. Port is randomly selected and communications encrypted with TLS 1.2.
53202	TCP	WSD Transfer
53303	TCP	WSD Print
53404	TCP	WSD Scan

Network Encryption

IPSec

Internet Protocol Security (IPsec) is a network security protocol capable of providing encryption and authentication at the packet level. VersaLink® products support IPSec for both IPv4 and IPv6 protocols.

		VersaLink® Multifunction	VersaLink® Printers
		B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
IPSec			
	Supported IP Versions	IPv4, IPv6	IPv4, IPv6
	Key exchange authentication method	Preshared Key & digital signature	Preshared Key & digital signature
	Transport Mode	Transport mode only	Transport mode only
	Security Protocol	ESP only	ESP only
	ESP Encryption Method	AES, 3DES, DES	AES, 3DES, DES
	ESP Authentication Methods	SHA1, SHA256, None	SHA1, SHA256, None

Wireless 802.11 Wi-Fi Protected Access (WPA)

Products equipped with WiFi support WPA2 Personal, WPA2 Enterprise, and Mixed Mode compliant with IEEE 802.11i. The wireless network adapters used in Xerox products are certified by the Wi-Fi Alliance.

		VersaLink® Multifunction	VersaLink® Printers
		B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Wi-Fi (802.11)			
	No Encryption	Supported	Supported
	WEP	RC4	RC4
	WPA2 Personal (PSK)	CCMP (AES)	CCMP (AES)
	WPA2 Enterprise	CCMP (AES) + TKIP -- PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/CHAP EAP-TTLS/MS-CHAPv2	CCMP (AES) + TKIP -- PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/CHAP EAP-TTLS/MS-CHAPv2
	BSSID Roaming Restriction	(Not Currently Supported)	(Not Currently Supported)

TLS

VersaLink® products support the latest version, TLS 1.2.

	VersaLink® Multifunction	VersaLink® Printers	
	B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000	
TLS Versions Supported			
	Product Web Interface	1.2, 1.1, 1.0	1.2, 1.1, 1.0
	Product Web Services	1.2, 1.1, 1.0	1.2, 1.1, 1.0
	Product IPPS printing	1.2, 1.1, 1.0	1.2, 1.1, 1.0
	Remote control	1.2	1.2

Public Key Encryption (PKI)

A digital certificate is a file that contains data used to verify the identity of the client or server in a network transaction. A certificate also contains a public key used to create and verify digital signatures. To prove identity to another product, a product presents a certificate trusted by the other product. The product can also present a certificate signed by a trusted third party and a digital signature proving that it owns the certificate.

A digital certificate includes the following data:

- Information about the owner of the certificate
- The certificate serial number and expiration date
- The name and digital signature of the certificate authority (CA) that issued the certificate
- A public key
- A purpose defining how the certificate and public key can be used
- There are four types of certificates:
 - A Product Certificate is a certificate for which the printer has a private key. The purpose specified in the certificate allows it to be used to prove identity.
 - A CA Certificate is a certificate with authority to sign other certificates.
 - A Trusted Certificate is a self-signed certificate from another product that you want to trust.
 - A domain controller certificate is a self-signed certificate for a domain controller in your network. Domain controller certificates are used to verify the identity of a user when the user logs in to the product using a Smart Card.

For protocols such as HTTPS, the printer is the server, and must prove its identity to the client Web browser. For protocols such as 802.1X, the printer is the client, and must prove its identity to the authentication server, typically a RADIUS server.

Device Certificates

VersaLink® products support both CA signed and self-signed certificates. Product certificates support a bit length of up to 2048 bits.

A CA signed certificate can be created by generating a Certificate Signing Request (CSR), and sending it to a CA or a local server functioning as a CA to sign the CSR. An example of a server functioning as a certificate authority is Windows Server 2008 running Certificate Services. When the CA returns the signed certificate, install it on the printer.

Alternatively, a self-signed certificate may be created. When you create a Product Certificate, the product generates a certificate, signs it, and creates a public key used in SSL/TLS encryption.

	VersaLink® Multifunction	VersaLink® Printers
	B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Device Certificates		
Certificate Length	1024, 2048	1024, 2048
Supported Hashes	SHA256, SHA384, SHA512	SHA256, SHA384, SHA512
Product Web Server	Supported	Supported
IPPS (TLS) Printing	Supported	Supported
802.1X Client	Supported	Supported
Email Signing	Supported	(Not Applicable)
Email Encryption	Supported	(Not Applicable)
OCSP Signing	Supported	Supported
IPSec	(Not currently supported)	(Not currently supported)
SFTP	(Not currently supported)	(Not Applicable)

Trusted Certificates

Public certificates may be imported to the product's certificate store for validation of trusted external products. The following categories are supported:

- A Trusted Root CA Certificate is a certificate with authority to sign other certificates. These certificates usually are self-signed certificates that come from another product or service that you want to trust.
- An Intermediate CA Certificate is a certificate that links a certificate to a Trusted Root CA Certificate in certain network environments.
- Other Certificates are certificates that are installed on the printer for solution-specific uses.

An administrator can specify the minimum encryption key length required for certificates. If a user attempts to upload a certificate that contains a key that does not meet this requirement, a message appears. The message alerts the user that the certificate they are attempting to upload does not meet the key length requirement.

	VersaLink® Multifunction	VersaLink® Printers
	B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Trusted Certificates		
Minimum Length Restriction Options	1024, 2048	1024, 2048
Maximum Length	4096	4096
Supported Hashes	SHA1/224/256/384/512	SHA1/224/256/384/512
Supported Formats	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)	.cer, .der, PKCS#7, PKCS#12 (.pfx, .p12)
IPSec	Supported	Supported
LDAP	Supported	Supported
Scanning (HTTPS/TLS)	(Not currently supported)	(Not Applicable)
Scanning (SFTP/SSH)	(Not currently supported)	(Not Applicable)
802.1X Client	Supported	Supported
Email Signing	Supported	(Not Applicable)
Email Encryption	Supported	(Not Applicable)
OCSP Signing	Supported	Supported

Certificate Validation

VersaLink® devices support certificate validation with configurable checks for OSCP and CRL.

Validation checks include:

- Validation of certificate path
- Certificate expiration
- Validation of trusted CA
- Signature validation

Email Signing and Encryption using S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) provides Authentication, Message integrity, Non-repudiation, and encryption of email.

		VersaLink® Multifunction	VersaLink® Printers
		B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Email S/MIME			
	Versions	v2, v3, v3.2	(Not Applicable)
	Digest	MD5, SHA1, SHA256	(Not Applicable)
	Encryption	3DES, RC2, AES128, AES192, AES256	(Not Applicable)

SNMPv3

SNMPv3 is the current standard version of SNMP defined by the Internet Engineering Task Force (IETF). It provides three important security features:

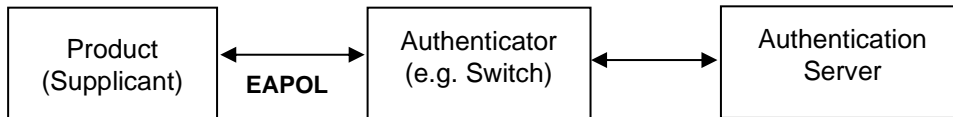
- Message integrity to ensure that a packet has not been tampered with in transit
- Authentication to verify that the message is from a valid source
- Encryption of packets to prevent unauthorized access

		VersaLink® Multifunction	VersaLink® Printers
		B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
SNMPv3			
	Digest	SHA1, MD5	SHA1, MD5
	Encryption	DES, AES128	DES, AES128

Network Access Control

802.1x

In 802.1X authentication, when the product is connected to the LAN port of Authenticator such as the switch as shown below, the Authentication Server authenticates the product, and the Authenticator controls access of the LAN port according to the authentication result. The product starts authentication processing at startup when the startup settings for 802.1X authentication are enabled.



	VersaLink® Multifunction	VersaLink® Printers
	B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Network Access Control		
	802.1x	Supported
	Authentication Methods	MD5, MS-CHAPv2, PEAP/MS-CHAPv2, EAP-TLS
		Supported
		MD5, MS-CHAPv2, PEAP/MS-CHAPv2, EAP-TLS

Cisco Identity Services Engine (ISE)

Cisco ISE is an intelligent security policy enforcement platform that mitigates security risks by providing a complete view of which users and what products are being connected across the entire network infrastructure. It also provides control over what users can access your network and where they can go. Cisco's ISE includes over 200 Xerox product profiles that are ready for security policy enablement. This allows ISE to automatically detect Xerox products in your network. Xerox products are organized in Cisco ISE under product families, such as VersaLink® products, enabling Cisco ISE to automatically detect and profile new Xerox products from the day they are released. Customers who use Cisco ISE find that including Xerox products in their security policies is simpler and requires minimal effort.

Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. ISE collects various attributes for each network endpoint to build an endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of product profiles. These profiles include a wide range of product types, including tablets, smartphones, cameras, desktop operating systems (for example, Windows®, Mac OS® X, Linux® and others), and workgroup systems such as Xerox printers and MFPs.

Once classified, endpoints can be authorized to the network and granted access based on their profile signature. For example, guests to your network will have different level of access to printers and other end points in your network. As an example, you and your employees can get full printer access when accessing the network from a corporate workstation but be granted limited printer access when accessing the network from your personal Apple® iPhone®.

Cisco ISE allows you to deploy the following controls and monitoring of Xerox products:

- Automatically provision and grant network access rights to printers and MFPs to prevent inappropriate access (including automatically tracking new printing products connecting to the network):
 - Block non-printers from connecting on ports assigned to printers
 - Prevent impersonation (aka spoofing) of a printer/MFP
 - Automatically prevent connection of non-approved print products
 - Smart rules-based policies to govern user interaction with network printing products
- Provide simplified implementation of security policies for printers and MFPs by:
 - Providing real time policy violation alerts and logging
 - Enforcing network segmentation policy
 - Isolating the printing products to prevent general access to printers and MFPs in restricted areas
- Automated access to policy enforcement
 - Provide extensive reporting of printing product network activity

		VersaLink® Multifunction	VersaLink® Printers
		B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Network Access Control			
	Cisco ISE	Supported	Supported

Contextual Endpoint Connection Management

Traditionally network connection management has been limited to managing endpoints by IP address and use of VLANs and firewalls. This is effective, but highly complex to manage for every endpoint on a network. Managing, maintaining, and reviewing the ACLs (and the necessary change management and audit processes to support them) quickly become prohibitively expensive. It also lacks the ability to manage endpoints contextually.

Connectivity of VersaLink® devices can be fully managed contextually by Cisco TrustSec. TrustSec uses Security Group Tags (SGT) that are associated with an endpoint's user, device, and location attributes. SG-ACLs can also block unwanted traffic so that malicious reconnaissance activities and even remote exploitation from malware can be effectively prevented.

FIPS140-2 Compliance Validation

When enabled, the product will validate its current configuration to identify cryptographic modules in use. Modules which are not FIPS 140-2 (Level 1) compliant will be reported.

VersaLink® products use encryption algorithms for Kerberos, SMB, SNMPv3, and PDF Direct Print Service that are not approved by FIPS140-2. They can however operate in FIPS140-2 approved Mode in order to maintain compatibility with conventional products after an exception is approved by a system administrator. They do not use FIPS compliant algorithms when in this configuration.

Additional Network Security Controls

Endpoint Firewall Options

	VersaLink® Multifunction	VersaLink® Printers
	B405, B605, B615, B7025, B7030, B7035, C405, C505, C605, C7020, C7025, C7030	B400, B600, B610, C400, C500, C600, C7000, C8000, C9000
Firewall	IP Whitelisting	IP Whitelisting
Stateful Firewall	(Not currently supported)	(Not currently supported)
IP Whitelist	Supported	Supported

IP Whitelisting (IP Address Filtering)

VersaLink® products support Whitelisting only

When enabled all traffic is prohibited regardless of interface (wired/wireless) unless enabled by IP filter rule. IPv4 and IPv6 are enabled separately. If IP Filter and IPsec are both enabled, IPsec is evaluated first. Up to 25 addresses can be enabled for IPv4 and an additional 25 for IPv6. Addresses include IP and subnet allowing individual system or subnets to be enabled. A system administrator can disable this feature using the embedded web server.

Stateful Firewall (Advanced IP Filtering)

VersaLink® products do not support Stateful Firewall.

Personal Identifiable Information (PII)

Personal Identifiable Information (PII) can be entered or stored into the device through several means: address book, scan templates, device description, display device information, audit logs, and engineering logs. The PII is encrypted on the device so not readable outside of the operation of the device. The Admin controls the ability of users to enter data, and controls the accessibility of logs, or the deletion of logs. If users wish not to have any PII stored on the device, the Admin has the ability to restrict the features where PII could be stored and has the ability to restrict access to logs. Users do not have access to the internals of the device (memory, hard drive) where PII may be resident.

6. Device Security: BIOS, Firmware, OS, Runtime, and Operational Security Controls

VersaLink® products have robust security features that are designed to protect the system from a wide range of threats. Below is a summary of some of the key security controls.

Pre-Boot BIOS Protection

BIOS

- The BIOS is inaccessible and cannot be cleared or reset.
- The BIOS can only be modified by a firmware update, which is digitally signed.
- BIOS will fail secure, locking the system if integrity is compromised.

Embedded Encryption

- Configuration Settings (including security settings) and User Data are encrypted by AES.
- Each device is encrypted using its own unique key.

Boot Process Integrity

Firmware Integrity & Verification

- Firmware is digitally signed.
- Firmware is verified against a whitelist using cryptographic hashing.

Event Monitoring & Logging

- The Audit Log feature records security-related events.

Runtime Security

VersaLink® does not support McAfee Embedded Control.

Event Monitoring and Logging

- The Audit Log feature records security-related events.

Continuous Operational Security

Firmware and Diagnostic Security Controls

- Firmware installation controls limit who can install firmware and from where.

- Customer defined service technician (CSE) restrictions add an additional layer of protection to prevent unauthorized access and/or modification of VersaLink® products.
- Continuous logging

Fail Secure Vs Fail Safe

VersaLink® products are designed to fail secure.

When a security control is compromised, the control is no longer trustworthy, and a system is at risk of further compromise. In such a scenario, security products may either fail safe [open] or fail secure [closed].

An example from physical security is a door. If power is lost the door may either:

- Unlock and 'fail safe' to an open state (likely for safety reasons such as in a public building).
- Lock and 'fail secure' for security reasons (such as a bank vault).

Pre-Boot Security

BIOS

The BIOS used in VersaLink® products is embedded and cannot be accessed directly. Unlike devices such as Desktop and Laptop computers that have a BIOS that can be accessed via a keystroke on startup, the BIOS of VersaLink® products it's not accessible.

Many devices can be cleared to factory defaults (including passwords and security settings) by depressing a reset button using a paperclip or similar method. For security reasons, VersaLink® products do not offer such a method to clear or reset the BIOS. (Note that configuration settings may be reset to factory defaults by an authorized administrator, however this does not impact BIOS settings).

BIOS updates are not applied by device firmware updates. Firmware is protected from tampering by use of digital signatures (discussed later in this section).

The BIOS is designed to fail secure. An integrity check is performed immediately when power is applied. If verification is successful, the system proceeds with OS kernel boot. If the integrity check fails, the system will fail secure.

Embedded Encryption

AES encryption is used to protect the system, user data, and configuration (including security settings) from being retrieved or modified. Each device uses its own unique key that is securely generated. Encryption is enabled by default. Media encryption and sanitization are discussed in Section 3 User Data Protection.

Boot Process Security

Firmware Integrity

Unlike open operating systems such as servers and user workstations in which software may be installed by users, Xerox products are based on embedded systems and the contents are managed by Xerox. The only means of modifying the contents of a device is by applying a firmware update package.

Firmware updates use a special format and each firmware update is digitally signed to protect the integrity of the contents. Firmware that is corrupt or has been illicitly modified will be rejected. **This security control cannot be disabled.**

VersaLink® products include a built-in firmware software validation. This is a file integrity monitor that compares the security hashes of currently installed firmware to a secured whitelist that was installed when the signed firmware was installed.

Event Monitoring and Logging

Audit Log

The Audit Log feature records security-related events. The Audit Log contains the following information:

Field	Description
Index	A unique value that identifies the event.
Date	The date that the event happened in mm/dd/yy format.
Time	The time that the event happened in hh:mm:ss format.
ID	The type of event. The number corresponds to a unique description.
Description	An abbreviated description of the type of event.
Additional Details	Columns 6–10 list other information about the event, such as: Identity: User Name, Job Name, Computer Name, Printer Name, Folder Name, or Accounting Account ID display when Network Accounting is enabled. Completion Status Image Overwrite Status: The status of overwrites completed on each job. Immediate Image must be enabled.

VersaLink® products currently support 52 unique events.

A maximum of 15,000 events can be stored on the device. When the number of events exceeds 15,000, audit log events will be deleted in order of timestamp, and then new events will be recorded. The audit log can be exported at any time by a user with administrative privileges. Note that as a security precaution, audit log settings and data can only be accessed via HTTPS.

Operational Security

Firmware Restrictions

The list below describes supported firmware delivery methods and applicable access controls.

- **Local Firmware Upgrade via USB port:**
Xerox service technicians can update product firmware using a USB port and specially configured USB thumb drive. This ability can be restricted by enabling the Customer Service Engineer Restriction feature which will require entry of a unique, customer designated password in order to accept the update.
- **Network Firmware Update:**
Product system administrators can update product firmware using the Embedded Web Server. The ability to apply a firmware update is restricted to roles with system administrator or Xerox service permissions. Firmware updates can be disabled by a system administrator.
- **Xerox Remote Services Firmware Update:**
Xerox Remote Services can update product firmware securely over the internet using HTTPS. This feature can be disabled, scheduled, and includes optional email alerts for system administrators.

The programs stored in the Flash ROM listed below are downloadable from external sources.

- Controller
- Marking Engine
- Scanner
- Document Feeder
- Finisher (Option for processing printed paper. No description on Finisher is provided in this document because user's image data will not be stored in it.)
- High capacity feeder (No description on High capacity feeder is provided in this document because user's image data will not be stored in it.)
- High capacity stacker (No description on high capacity stacker is provided in this document because user's image data will not be stored in it.)
- Interface Module (No description on interface module is provided in this document because user's image data will not be stored in it.)
 - This program-downloading function can be disabled by a system administrator from the local UI.
 - The header part of file is using software to identify whether the download file is legitimate.

Service Technician (CSE) Access Restriction

The CSE (Customer Service Engineer) Access Restriction allows customers to create an additional password that is independent of existing administrator passwords. This password must be supplied to allow service of the product. This password is not accessible to Xerox support and cannot be reset by Xerox service personnel.

Additional Service Details

Xerox products are serviced by a tool referred to as the Portable Service Workstation (PWS). Only Xerox authorized service technicians are granted access to the PWS. Customer documents or files cannot be accessed during a diagnostic session, nor are network servers accessible through this port. If a network connection is required while servicing a Xerox device, service technicians will remove the device from any connected networks. The technician will then connect directly to the device using an Ethernet cable, creating a physically secure and isolated network during service operations.

Backup and Restore (Cloning)

Certain system settings can be captured in a 'clone' file that may be applied to other systems that are the same model. Clone files are encoded but not encrypted and have the potential to contain sensitive information depending on which product feature setting is selected. Access to both create and apply a clone file can be restricted using role-based access controls. Clone files can only be created and applied through the Embedded Web Server.

EIP Applications

Xerox products can offer additional functionality through the Xerox Extensible Interface Platform® (EIP). Third party vendors can create Apps that extend the functionality of a product. Xerox signs EIP applications that are developed by Xerox or Xerox partners. Products can be configured to prevent installation of unauthorized EIP applications.

XCP (eXtensible Customizable Platform)

VersaLink® products offer additional functionality through the eXtensible Customizable Platform (XCP) plug-in interface. Plug-ins can alter current functionality and add new functionality that may impact the security of the product. XCP Plug-ins are signed and encrypted by Xerox; products can be configured to reject unsigned plug-ins. XCP plug-ins are used to support USB peripherals and alternative login methods (such as Smart Card login). The XCP plug-in feature is disabled by default and must be manually enabled by a system administrator using the embedded web server.

7. Configuration and Security Policy Management Solutions

Xerox Device Manager and Xerox® CentreWare® Web (available as a free download) centrally manage Xerox Devices.

For details please visit Xerox.com or speak with a Xerox representative.

8. Identification, Authentication, and Authorization

VersaLink® products offer a range of authentication and authorization options to support various environments.

Single Factor authentication is supported locally on the product or via external network authentication servers (e.g., LDAP, Kerberos, ADS). Multi Factor authentication is supported by addition of card reader hardware. (Where ease of access is desired, open access and simple user identification modes also exist, however these are not recommended for secure environments.)

In all modes, product administrator accounts always require authentication. This cannot be disabled.

A flexible RBAC (Role Based Access Control) security model supports granular to assign of user permissions. Once a user has been authenticated, the product grants (or denies) user permissions based upon the role(s) they have been assigned to. Pre-defined roles that may be used or custom roles may be created as desired.

Authentication

VersaLink® devices support the following authentication mode:

- Local Authentication
- Network Authentication
- Smart Card Authentication (CAC, PIV, SIPR, .Net)
- Convenience Authentication

Local Authentication

The local user database stores user credential information. The printer uses this information for local authentication and authorization, and for Xerox® Standard Accounting. When you configure local authentication, the printer checks the credentials that a user provides against the information in the user database. When you configure local authorization, the printer checks the user database to determine which features the user is allowed access. Each device has a unique default administrator password which should be changed as soon as possible along with enabling recommended security features to secure the system.

Note: User names and passwords stored in the user database are not transmitted over the network

Password Policy

The following password attributes can be configured:

Password Policy	
Minimum Length	1
Maximum Length	63
Password cannot contain User Name	Supported
Password complexity options (in addition to alphabetic characters)	Require a number Requires non-alphabetic

Network Authentication

When configured for network authentication, user credentials are validated by a remote authentication server.

Network Authentication Providers	
Kerberos (Microsoft Active Directory)	Supported
Kerberos (MIT)	Supported
SMB NTLM Versions Supported	NTLMv2
LDAP Versions Supported	Version 3 (including TLS 1.2)

Smart Card Authentication

Two-factor security – Smart Card plus User Name/Password combination. Requires optional card reader hardware and software plugin. Authentication is handled by a remote server. Supported remote authentication methods include Kerberos, SMB and LDAP.

Smart Card authentication is considered very secure due to the nature of the Smart Card architecture and potential levels of encryption of data on the card itself.

Support for the SIPR network is provided using the XCP Plug-in architecture and a Smart Card authentication solution created by 90meter under contract for Xerox.

Details regarding 90meter can be found online here: <https://www.90meter.com/>

Other Smart Card authentication solutions are offered including support for CAC/PIV and .NET compatible cards leveraging XCP Plug-ins.

Smart Cards	
Common Access Card (CAC)	Supported
PIV / PIV II	Supported
Net (Gemalto .Net v1, Gemalto .Net v2)	Supported
Gemalto MD	Not Currently Supported

Convenience Authentication

Convenience authentication offloads authentication to a third-party solution which may offer more or less security than native security implementations. Users swipe a pre-programmed identification card or key fob to access the device.

For example, employees may be issued key fobs for access to facilities. Convenience mode may be configured to allow an employee to authenticate using their fob or require the fob in a multi-factor manor. The level of security provided is dependent upon the chosen implementation.

Some examples of third party convenience authentication providers include:

- Pharos print management solutions: <https://pharos.com/>
- YSoft SafeQ: <https://www.ysoft.com/en>

Contact your Xerox sales representative for details and other options.

Simple Authentication (non-secure)

Simple authentication is mentioned here for completeness. It is intended for environments where authentication is not required. It is used for customization only. When in this mode, users are not required to enter a password. (The device administrator account always requires a password).

Authorization (Role Based Access Controls)

VersaLink® products offer granular control of user permissions. Users can be assigned to pre-defined roles or customers may design highly flexible custom permissions. A user must be authenticated before being authorized to use the services of the product. Authorization ACLs (Access Control Lists) are stored in the local user database. Authorization privileges (referred to as permissions) can be assigned on a per user or group basis.

Please note that Xerox products are designed to be customizable and support various workflows as well as security needs. User permissions include security-related permissions and non-security related workflow permissions (e.g., walkup user options, copy, scan, paper selection, etc.). Only security-related permissions are discussed here.

Remote Access

Without RBAC permissions defined basic information such as Model, Serial number, and Software Version can be viewed by unauthenticated users. This can be disabled by restricting access to the device website pages for non-logged-in users.

By default, users are allowed to view basic status and support related information, however they are restricted from accessing device configuration settings. Permission to view this information can be disallowed.

Local Access

Without RBAC permissions defined basic information such as Model, Serial number, Software Version, IP address, and Host Name can be viewed without authentication. This can be disabled by disallowing access to device settings for unauthenticated.

By default, users are allowed to access the local interface, however they are restricted from accessing device configuration settings. Roles can be configured to allows granular access to applications, services, and tools. Users can be also restricted from accessing the local interface completely.

9. Additional Information and Resources

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see <https://www.xerox.com/security>.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: <https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html>

Additional Resources

Below are additional resources.

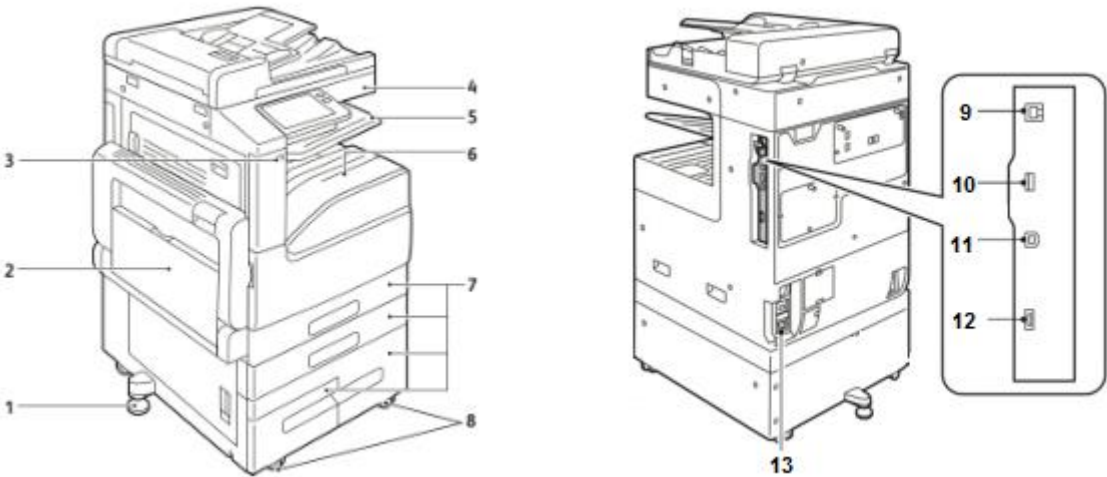
Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/

10. Appendix A: Product Security Profiles

This appendix describes specific details of each VersaLink® product.

VersaLink B7025/B7030/B7035

Physical Overview



- | | |
|--|---|
| <ul style="list-style-type: none">1. Stabilizer2. Bypass paper feed tray3. USB2.0 (Host Type A)*4. Touch screen user interface.5. Upper paper tray6. Lower paper tray7. Paper feed trays | <ul style="list-style-type: none">8. Caster wheels9. USB3.0 (Target Type B)*10. Optional Wi-Fi dongle port*11. RJ45 Ethernet connection*12. Debug serial port (DIN)*
(Located under steel plate)13. AC Power |
|--|---|

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
	N/A	Optional	N/A	Internal
Contains User Data (e.g., Print, Scan, Fax)	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
Customer Erasable	N/A	Factory Reset	N/A	Factory Reset

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board

HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk

SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
2GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Marking Engine Non-Volatile Storage

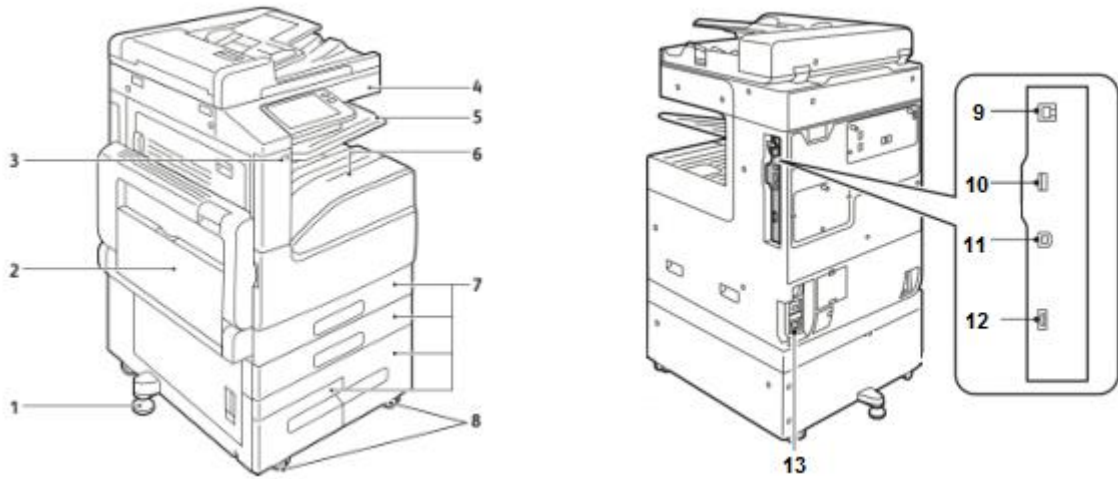
N/A. The marking engine does not contain any non-volatile storage.

Marking Engine Volatile Memory

N/A. The marking engine volatile memory does not store or process user data.

VersaLink C7000/C7020/C7025/C7030

Physical Overview



- | | |
|---------------------------------|---|
| 1. Stabilizer | 8. Caster wheels |
| 2. Bypass paper feed tray | 9. USB3.0 (Target Type B)* |
| 3. USB2.0 (Host Type A)* | 10. Optional Wi-Fi dongle port* |
| 4. Touch screen user interface. | 11. RJ45 Ethernet connection* |
| 5. Upper paper tray | 12. Debug serial port (DIN)*
(Located under steel plate) |
| 6. Lower paper tray | 13. AC Power |
| 7. Paper feed trays | |

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
	N/A	Optional	N/A	Internal
Contains User Data (e.g., Print, Scan, Fax)	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
Customer Erasable	N/A	Factory Reset	N/A	Factory Reset

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
2/4GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Marking Engine Non-Volatile Storage

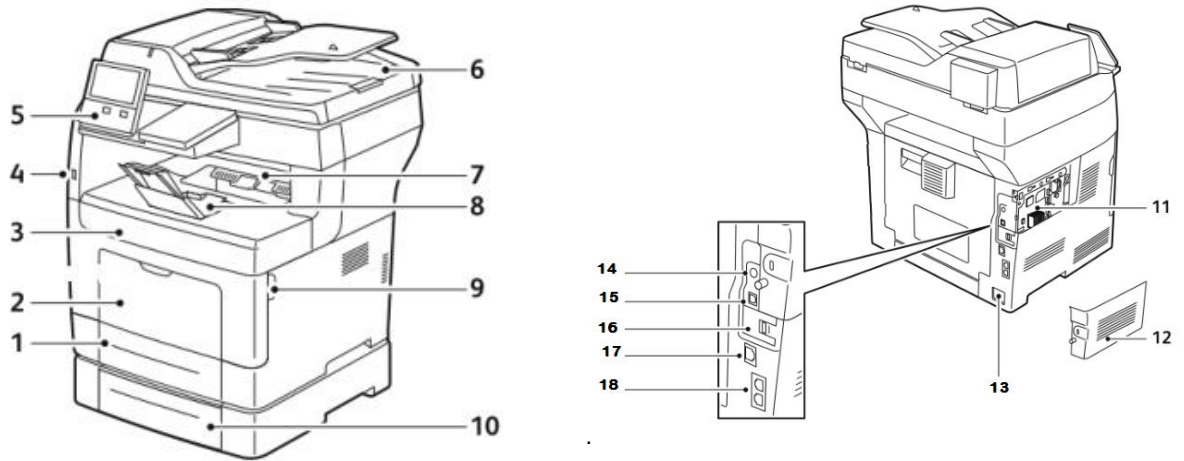
N/A. The marking engine does not contain any non-volatile storage.

Marking Engine Volatile Memory

N/A. The marking engine volatile memory does not store or process user data.

VersaLink B400/B405

Physical Overview



- | | |
|--|---|
| 1. Upper Paper Tray | 10. Lower Paper Tray |
| 2. Special Paper Feed | 11. Optional SSD Install Location |
| 3. Front Bezel | 12. SSD Install Location Cover |
| 4. USB 2.0 (A) | 13. AC Power |
| 5. Touch Screen User Interface , Power Button and Optional NFC | 14. Foreign Device Interface |
| 6. Document Feeder | 15. USB 3.0 (B) |
| 7. Catch Tray | 16. Optional Wireless Adapter Connector |
| 8. Catch Tray Extension | 17. RJ-45 Ethernet Connector |
| 9. Jam Clearance Open | 18. RJ-11 Fax and Telephone Connector |

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
	N/A	N/A	Optional	Internal
Contains User Data (e.g., Print, Scan, Fax)	Yes	N/A	Yes	N/A
Encryption Support	Always-On	N/A	Always-On	N/A
NIST 800-171 Overwrite Support	Yes	N/A	Yes	N/A
Contains Configuration Settings	Yes	N/A	Yes	N/A
Encryption Support	Always-On	N/A	Always-On	N/A
Customer Erasable	Factory Reset	N/A	Factory Reset	N/A

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
2GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Marking Engine Non-Volatile Storage

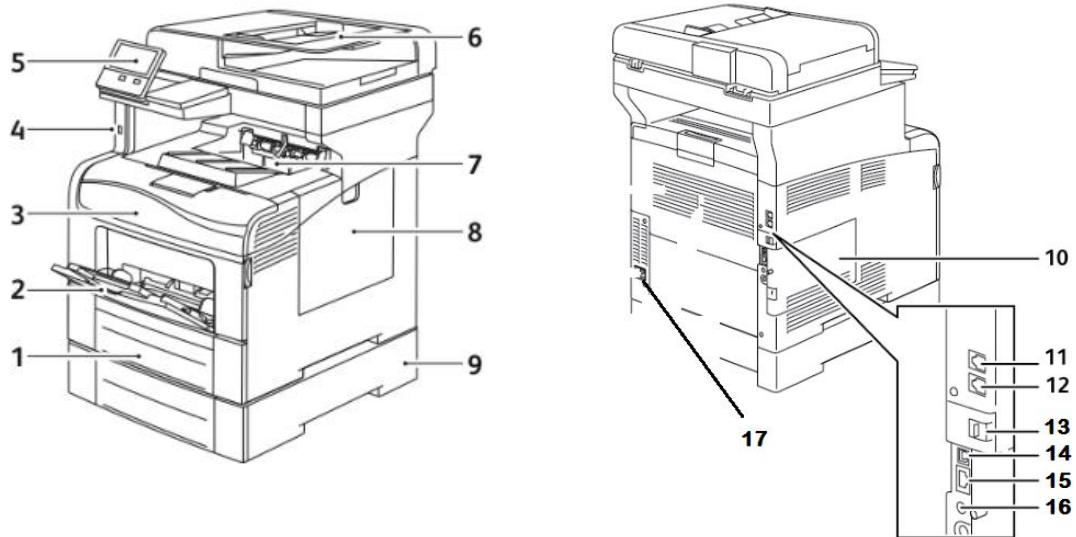
N/A. The marking engine does not contain any non-volatile storage.

Marking Engine Volatile Memory

N/A. The marking engine volatile memory does not store or process user data.

VersaLink C400/C405

Physical Overview



- | | |
|---|---|
| 1. Upper Paper Tray | 9. Lower Paper Tray |
| 2. Special Paper Feed | 10. Service Panel |
| 3. Front Bezel | 11. RJ-11 Fax and Telephone Connector |
| 4. USB 2.0 (A) | 12. RJ-11 Fax and Telephone Connector |
| 5. Touch Screen User Interface, Power Button and Optional NFC | 13. Optional Wireless Adapter Connector |
| 6. Document Feeder | 14. USB 3.0 (B) |
| 7. Catch Tray | 15. RJ-45 Ethernet Connector |
| 8. Side Panel | 16. Foreign Device Interface |
| | 17. AC Power |

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
	N/A	N/A	Optional	Internal
Contains User Data (e.g., Print, Scan, Fax)	Yes	Yes	N/A	N/A
Encryption Support	Always-On	Always-On	N/A	N/A
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	Yes	Yes	N/A	N/A
Encryption Support	Always-On	Always-On	N/A	N/A
Customer Erasable	Factory Reset	Factory Reset	N/A	N/A

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
2GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Marking Engine Non-Volatile Storage

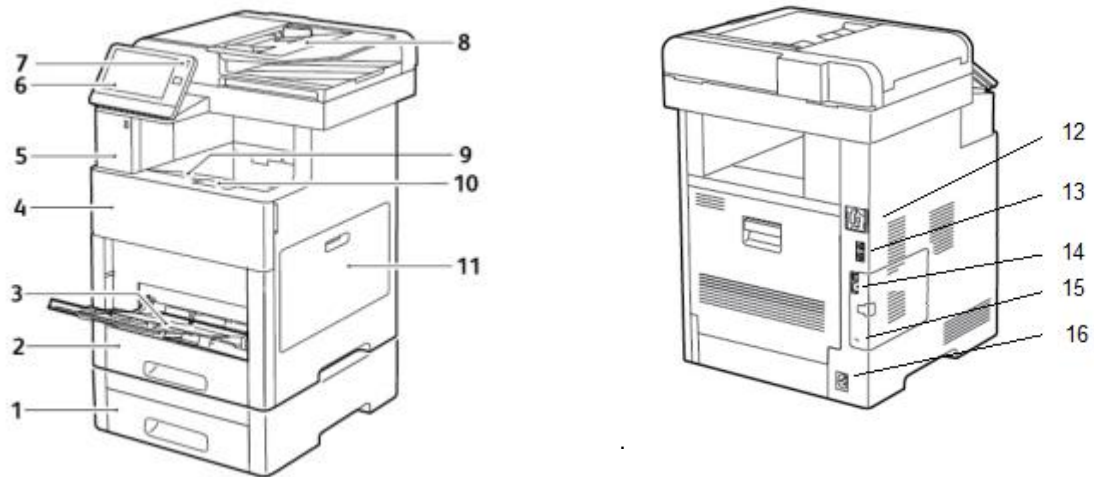
N/A. The marking engine does not contain any non-volatile storage.

Marking Engine Volatile Memory

N/A. The marking engine volatile memory does not store or process user data.

VersaLink C500/C600/C505/C605

Physical Overview



- | | |
|--|---|
| <ol style="list-style-type: none">1. Paper feed tray.2. Paper feed tray.3. Bypass paper feed tray.4. Front bezel.5. USB2.0(A).6. Touch screen user interface.7. System power button.8. Document feeder. | <ol style="list-style-type: none">9. Document output tray.10. Document output tray extension.11. Jam clearance panel.12. Optional Wi-Fi dongle connection.13. RJ11 Fax14. USB3.0 (B) & RJ45 Ethernet connection.15. Foreign device interface.16. AC Power. |
|--|---|

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
	N/A	N/A	Optional	Internal
Contains User Data (e.g., Print, Scan, Fax)	Yes	Yes	N/A	N/A
Encryption Support	Always-On	Always-On	N/A	N/A
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	Yes	Yes	N/A	N/A
Encryption Support	Always-On	Always-On	N/A	N/A
Customer Erasable	Factory Reset	Factory Reset	N/A	N/A

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
2/4GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Marking Engine Non-Volatile Storage

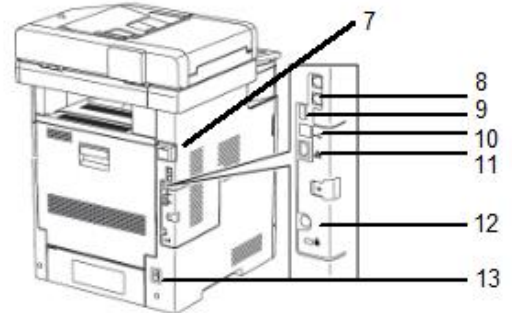
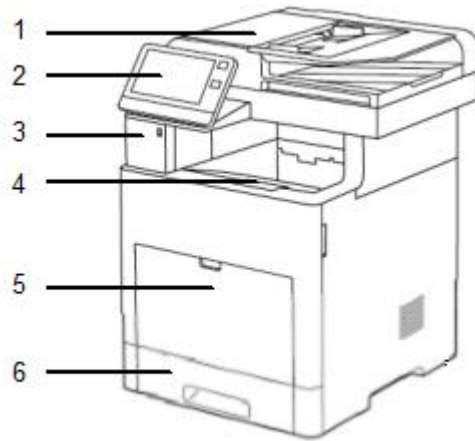
N/A. The marking engine does not contain any non-volatile storage.

Marking Engine Volatile Memory

N/A. The marking engine volatile memory does not store or process user data.

VersaLink B600/B605/B610/B615

Physical Overview



- | | |
|--|--|
| <ol style="list-style-type: none">1. Document feeder.2. Touch screen user interface.3. USB2.0(A).4. Document output tray.5. Bypass paper feed.6. Paper tray | <ol style="list-style-type: none">7. Optional Wi-Fi dongle connection.8. Optional RJ11 Fax9. USB2.0(A)10. USB3.0(B)11. RJ45 Ethernet12. Foreign device interface.13. AC Power. |
|--|--|

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
	N/A	N/A	Optional	Internal
Contains User Data (e.g., Print, Scan, Fax)	Yes	Yes	N/A	N/A
Encryption Support	Always-On	Always-On	N/A	N/A
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	Yes	Yes	N/A	N/A
Encryption Support	Always-On	Always-On	N/A	N/A
Customer Erasable	Factory Reset	Factory Reset	N/A	N/A

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
2GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Marking Engine Non-Volatile Storage

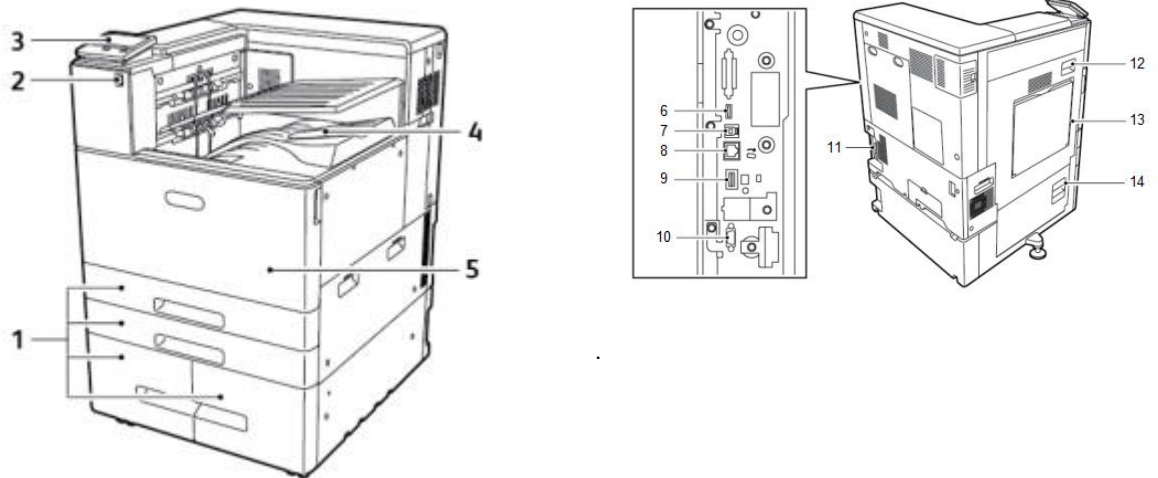
N/A. The marking engine does not contain any non-volatile storage.

Marking Engine Volatile Memory

N/A. The marking engine volatile memory does not store or process user data.

VersaLink C8000/C9000

Physical Overview



- | | |
|--|---|
| <ol style="list-style-type: none">1. Paper feed tray.2. USB2.0(A).3. Touch screen user interface.4. Document output tray.5. Jam clearance panel.6. USB2.0(A).7. USB3.0(B). | <ol style="list-style-type: none">8. RJ45 Ethernet connection.9. Optional Wi-Fi dongle connection.10. Foreign device interface.11. AC Power.12. Jam clearance panel.13. Special paper tray.14. Jam clearance panel. |
|--|---|

Security Related Interfaces

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front Panel Optional USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently or restricted using role based access controls. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

Encryption and Overwrite

Encryption and Overwrite	
Encryption	AES-256
TPM Chip	TPM chip is standard and cannot be disabled.
Media Sanitization	Immediate and On-Demand Image Overwrite.

Controller Non-Volatile Storage

	IC	HDD	SSD	SD Card
	N/A	N/A	Optional	Internal
Contains User Data (e.g., Print, Scan, Fax)	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
NIST 800-171 Overwrite Support	N/A	Yes	N/A	N/A
Contains Configuration Settings	N/A	Yes	N/A	Yes
Encryption Support	N/A	Always-On	N/A	Always-On
Customer Erasable	N/A	Factory Reset	N/A	Factory Reset

Note: Configuration settings may be erased by the reset to factory defaults feature.

IC- Integrated Circuit, soldered to circuit board
HDD- Magnetic Hard Disk Drive

SSD- Solid State Disk
SD Card- Secure Digital Card

Controller Volatile Memory

Size	Type	Use	User Data	How to Clear	Volatile
4GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

Marking Engine Non-Volatile Storage

N/A. The marking engine does not contain any non-volatile storage.

Marking Engine Volatile Memory

N/A. The marking engine volatile memory does not store or process user data.

11. Appendix B: Security Events

Xerox VersaLink Security Events

ID	Event	Description
101	Started normally (cold boot)	
101	Started normally (warm boot)	
101	Started (NVM initialized)	
101	Started (Hard Disk initialized)	
101	Shutdown requested	
101	Image Overwriting started	Completion: ("Success" / "Failed") Scheduled On Demand
101	Image Overwriting finished	Completion: ("Success" / "Failed")
101	Self-Test	Completion: ("Success" / "Failed") Checksum of ROM image 1 Checksum of ROM image 2
201	Login	User name Completion: ("Success" / "Failed Invalid User ID" / "Failed Invalid Password" / "Failed") Host Name or IP Address Method: ("Local" / "Remote" / "Convenience" , "Custom") Role: ("System Administrator" / "Customer Engineer" / "Casual Operator")
201	Logout	User name Completion: ("Success" / "Failed")
201	Locked System Administrator Authentication	Count of Remaining Authentication Failures
201	Detected Continuous Authentication Fail	User name Protocol: ("SNMPv3" / "EWS") Count of Remaining Authentication Failures
301	Audit Log	User name Completion: ("Enabled" / "Disabled")

ID	Event	Description
401	Print	User name Completion: ("Completed" / "Completed with Warnings" / "Cancelled by User" / "Cancelled by Shutdown" / "Aborted" / "Unknown") Root Job UUID Relation: ("Related" / "Owned") Job Accounting ID Action Details Host Name or IP Address File Name
401	Copy	Action Details
401	Scan	Encrypted, Signed, Destination Name, Sender Name
401	Fax	Action Details, Destination Name, Sender Name
401	Mailbox	Action Details
401	Print Reports	
401	Job Flow Service	
501	Adjust Time	Completion: ("Success" / "Failed")
501	Add User	User name User Role
501	Edit User	User name User Role ID Password CardID Name Permission Role ICCardID Other
501	Delete User	User Name
501	Create Mailbox	Host Name or IP Address Box Number
501	Delete Mailbox	
501	Switch Authentication Mode	Completion: ("Success") New Setting Previous Setting

ID	Event	Description
501	Change Security Setting	Authentication Accounting Image Overwrite HDD Encryption SSL S/MIME IPSEC SNMPv3 802.1x Certificate Verify Mode Maintainer Password SmartCard FIPS140 Self Test Auto Clear Timer Service Rep. Restricted Operation Print Reports Button External Code Integrity Check Authorization NFC
501	View Security Setting	Access Method: ("Local" / "EWS") Host Name or IP Address
501	Change Contract Type	User name Completion: ("Success" / "Failed" / "Aborted")
501	Change Geographic Region	
501	Enter Activation Code	Completion: ("Success")
501	Change Job Setting	Completion: ("Success") Function Name: ("Delay Print" / "Private Print")
601	Change Billing Impression Mode	Completion: ("Success" / "Failed") Designated Mode ("A3 Mode" / "A4 Mode") Billing Meter Values
601	Import Certificate	User name Completion: ("Success" / "Failed") Category: ("RootCA" / "DeviceEE" / "SSCEE") Key Size Issuer DN Serial Number
601	Delete Certificate	
601	Add Address Entry	Host Name or IP Address Registration Number
601	Delete Address Entry	
601	Edit Address Entry	
601	Import Address Book	Host Name or IP Address
601	Export Address Book	

ID	Event	Description
601	Clear Address Book	Host Name or IP Address
601	Export Audit Log	
601	Install Custom Service	Completion: ("Failed") Host Name or IP Address Custom Service Name
601	Install Embedded Plug-in	Host Name or IP Address Plugin File Name
601	Export Cloning Data	Completion: ("Success" / "Failed") Category: ("Apps" / "Contacts" / "Connectivity" / "Permissions" / "System")
601	Import Cloning Data	
701	Important Parts	Completion: ("Replaced")
701	Hard Disk	Completion: ("Replaced" / "Installed" / "Removed")
701	Software	Completion: ("Updated") ROM Type: ("IOT" / "UI" / "Controller" / "FAX") New Version Previous Version
701	Trusted Communication	Completion: ("Failed") Protocol Name: ("SSL/TLS" / "IPSEC" / "S/MIME")

Xerox Security Incident Management

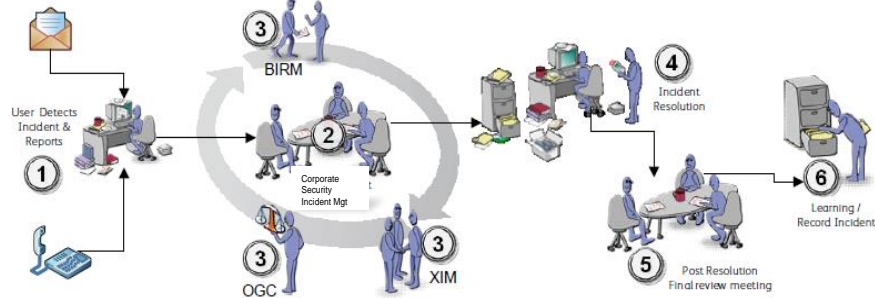
Xerox requires immediate reporting of potential security concerns through prescribed channels to enable prompt analysis, investigation and containment as needed to limit risk or loss.

Security Incident Examples

Physical/Personal Security	Electronic Security
<ul style="list-style-type: none">• Criminal activity• Harassment• Inappropriate use of email or internet• Pornography• Theft of data or information• Workplace violence• Loss of Customer Confidential Data	<ul style="list-style-type: none">• Application exploits• Compromised hosts• Denial of service attacks• Malware and viruses• Phishing attempts• Social media postings that can impact the reputation of Xerox• Incorrect postal or e-mail of customer data.

Xerox Security Incident Management Process Overview

Report > Respond > Contain > Communicate



Xerox Incident Management procedures are based on NIST 800-61 and aligned with corporate security policies as well as global ISO standards.



January 9, 2019

Ron Druzynski
Manager, Service Design
Engineering Services and
Support

Xerox Corporation
800 Phillips Road
Webster, NY 14580

Ronald.druzynski@xerox.com
tel 585.422-9393

Attestation of independent vulnerability/penetration testing

This document is intended to address any requests of Xerox's Engineering Services and Support (ESS) group to provide evidence of 3rd party vulnerability/penetration testing to external parties. The ESS ISO 27001-certified information security management system (ISMS) conforms to the international standard's independent review of information security control as well as complies with the related control defined in the Xerox corporate Information Security Policy (InfoSec 001). ESS implementation of these controls include internal and external ISO 27001 ISMS audits as well as penetration and vulnerability from external organizations on a regular basis.

ESS protects the results of all vulnerability assessments as we strive to diligently safeguard the confidentiality, integrity and availability of the information we manage for all of our customers. Per Xerox information classification policy this document is classified as Xerox Confidential. As a result, it is the policy of Xerox to not release the results of vulnerability assessments.

This letter serves to attest that ESS's last independent vulnerability/penetration assessment was performed:

Date: November 2017
Date of Report: December 28, 2017
Assessing Organization: Tag Solutions

The ESS ISMS is managed to review, risk assess and treat all found vulnerabilities in a timely manner.

If additional evidence of this assessment is desired, a controlled review of the related assessment report can be arranged.

Sincerely,

Ron Druzynski

AltaLink and VersaLink: Are compliant to the FAX requirement

AltaLink: Type A ports can be Disabled, Type B Ports cannot be Disabled but configured for one of two functions: Software Tools (Xerox Copier Assistant and Customer Utilities) and Direct Printing via Print Driver (USB memory Sticks are not supported).

VersaLink: Type A and Type B ports can be disabled

AltaLink and VersaLink: Hard Drives can be removed for a fee. For comparable effective data removal -> Full device reset back to FACTORY DEFAULT is available in addition to an On Demand Image Overwrite. Performing both would be an extremely effective data clearing method that requires no additional cost.

made
to
think.

Xerox® ConnectKey® Technology



THE ECOSYSTEM FOR WORKPLACE PRODUCTIVITY

xerox™

Your Workplace Assistant, Built on Xerox® ConnectKey® Technology

Today's workplace has evolved beyond the ability of any single machine to fulfill the productivity needs of the modern, mobile, always-connected workforce. Workplace assistants built on Xerox® ConnectKey Technology help businesses discover new ways to work smarter and create the most productive workplace. It's time to stop thinking about printers as standalone, task-specific workhorses, and start demanding more up-to-date, useful — and usable — solutions. Xerox® ConnectKey Technology delivers.



Each ConnectKey Technology-enabled printer and multifunction printer in our lineup becomes the center of a productivity ecosystem, bringing together all your devices, delivering an intuitive user experience, providing mobile and cloud connectivity, complete security and access to value-extending services right out of the box. You'll do more than print, scan or copy. You'll connect like never before.

XEROX® VERSALINK® PRINTER

Ideal for smaller workgroups in decentralized settings without full IT support, printers and multifunction printers in the VersaLink family are full-featured, app-centric workplace assistants. They provide an intuitive user experience and allow users to work whenever, from wherever.

XEROX® ALTALINK® PRINTER

With more performance and scalability for centralized, mid-size and larger workgroups, AltaLink multifunction printers deliver — with the advanced finishing options businesses need to boost output while reducing time spent on task.

Intuitive User Experience

Finally. Multifunction printers that work the way you expect them to — with a consistent user experience across the portfolio — and in perfect sync with the other devices you depend on to get work done.



KEEPING IT CONSISTENT

With a ConnectKey® Technology-enabled fleet — regardless of model — the user experience is always consistent. Common functions work similarly on every machine so users learn once and apply fleet-wide.

New installation wizards streamline setup to get you started with little or no IT support. Print drivers look and feel the same, while the Xerox® Global Print Driver® can be used on all machines regardless of model.

TOUCH, AND GO FAST.

The multi-touch experience — the way millions of phone and tablet users interact with today's most advanced devices — now finds its way to the printer or multifunction printer you'll depend on to get work done quickly and easily.

Swipe, tap and pinch your way through simplified workflows on a large, colorful, tablet-like screen. Download apps directly from the Xerox App Gallery and customize your interface to keep the apps you use most front and center. It's a completely new — and yet entirely familiar — way to power through complex workflows and common tasks.

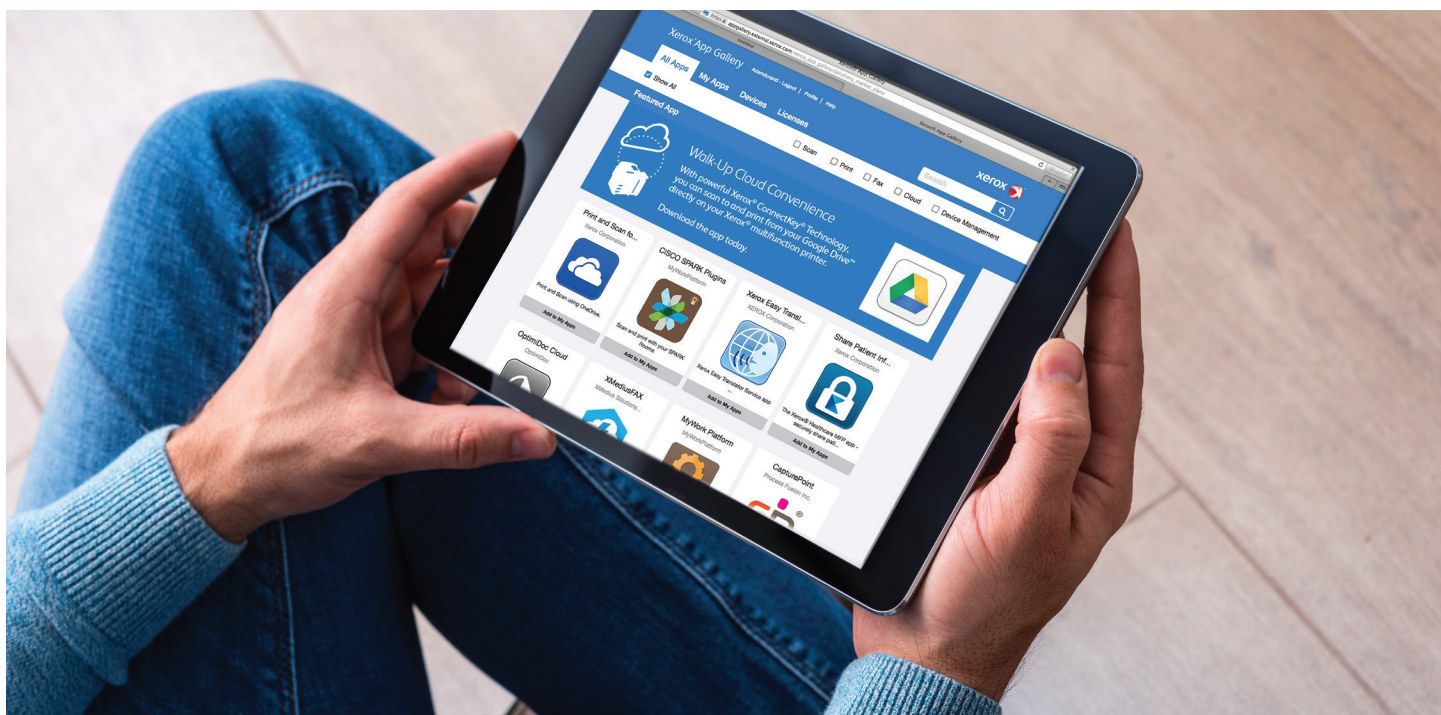
LET'S CUSTOMIZE.

With ConnectKey Technology's flexible design, device interfaces are customizable to provide only the apps you use most, including specific one-touch workflows to or from cloud or network locations.

And because ConnectKey Technology is built on an open systems architecture (Xerox Extensible Interface Platform®), even more customization is possible for highly specialized workflows.

Mobile and Cloud Ready

Your connected workforce — whether at home, on the road or in the office — relies on a variety of devices to do their jobs and on multiple remote locations from which to send or retrieve documents and information. Xerox® ConnectKey® Technology brings it all together.



READY FOR THE WAY YOU WORK

All ConnectKey Technology-enabled printers and multifunction printers give you the freedom to work where and how you want to — with access to Google Drive, Microsoft OneDrive, Dropbox, and additional options through the Xerox App Gallery.

The ability to connect and print from multiple devices is key for today's mobile worker, and ConnectKey multifunction printers are ready to roll with optional Wi-Fi® connectivity, front-panel-integrated Near Field

Communication (NFC) Tap-to-Pair, Apple® AirPrint® and native support for Google Cloud Print™, Xerox® Print Service for Android™ and Mopria®.

CONVENIENT, VERSATILE AND CLOUD-CONNECTED

With easy-to-use apps like Xerox® @printbyXerox App, printing to any ConnectKey Technology-enabled printer is as easy as sending an email with an attachment and retrieving it at any ConnectKey Technology-enabled device worldwide. It's easy, secure and free.

Scan or print directly to or from the cloud, easily share documents with individuals or groups without the hassle of multiple steps and create editable documents from hard copy source material. It's all possible, right from the device.

Benchmark Security

Security is a top priority for every business. Xerox® ConnectKey® Technology exceeds industry standards for security features and technologies. Work with total peace of mind.

A HIGHER STANDARD

Although it's integral to our technology, there's nothing standard about the levels of security included with every ConnectKey Technology-enabled device. Our holistic four-point approach to security ensures comprehensive and all-encompassing protection for all system components and points of vulnerability.

Prevent

ConnectKey Technology utilizes a comprehensive set of capabilities that prevents malicious attacks, the proliferation of malware and misuse of/unauthorized access to the printer, whether from transmitted data or direct interaction at the device.

All possible access points are secure, including the user interface and input ports accessible to walkup users as well as PC, server, mobile devices or cloud connections.

Detect

Xerox® ConnectKey Technology runs a comprehensive Firmware Verification test, either at start-up* or when activated by authorized users. This provides alerts if any harmful changes to the printer have been detected. McAfee® Whitelisting** technology constantly monitors for and automatically prevents any malicious malware from running.



Protect

Our comprehensive security measures don't stop with preventing unauthorized access to your printer and securing your information from the inside. ConnectKey® Technology provides capabilities to prevent intentional or unintentional transmission of critical data to unauthorized parties.

From protecting printed materials by not releasing documents until the right user is at the device, to preventing scanned information reaching beyond its intended recipient, ConnectKey Technology offers the safeguards you need to keep your most critical data assets safe and secure.

Xerox also protects all your stored information, using the highest levels of encryption. You can delete any processed or stored data that is no longer required using National Institute of Standards and Technology (NIST) and U.S. Department of Defense approved data clearing and sanitization algorithms***.

External Partnerships

ConnectKey Technology provides extra security standards through our partnership with McAfee*** and Cisco. We measure our performance against international standards with certifications like Common Criteria and FIPS 140-2 to ensure our devices are trusted in even the most secure environments.

A COMPREHENSIVE APPROACH TO SECURITY



Prevent
unauthorized access



Detect
suspicious or malicious behavior



Protect
data and documents



External Partnerships

* VersaLink® devices

** AltaLink® and iSeries devices

*** Applies to devices with hard disk drives only

Enables Next Generation Services

Combining Xerox® ConnectKey® Technology with Xerox® Intelligent Workplace Services creates an optimized infrastructure that is customized to your organization — whether it's large or small. Our state-of-the-art assessment tools and three-stage approach make sure you have the right mix of technology, apps and solutions.

ASSESS AND OPTIMIZE

With Xerox® ConnectKey Technology, you'll have powerful tools for ultimate control over every printer or multifunction printer in your network, including the ability to set job limits, monitor usage and perform backup and restoration operations. You'll gain more control over costs, reduce strain on IT resources and improve overall performance.

ConnectKey Technology-enabled devices are Cisco EnergyWise® compliant, so you can monitor and control energy usage across the fleet, or device by device. Set job limits with Xerox® Global Print Driver® and set material- and energy-saving print parameters with Earth Smart Printing. You'll reduce waste and power consumption while improving visibility to end-user printer usage.

SECURE AND INTEGRATE

You'll have comprehensive device, document and data security, with built-in protections that meet and exceed industry standards and government regulations.

Security measures include Encrypted Secure Print and Print Queue Deletion, Hard Disk Encryption and Disk Overwrite. Beyond on-device protections, your transmitted data is safer too, with Secure Email and Encryption, and powerful third-party protections like McAfee® Whitelisting*.

When it comes to mobile and cloud printing, ConnectKey Technology gives mobile and virtual workers a wide range of secure options to work from anywhere, anytime, including easy print support from tablets and mobile phones with support for Android™ devices and Apple® AirPrint®.

AUTOMATE AND SIMPLIFY

ConnectKey Technology-enabled devices, combined with MPS, accelerate the paper-to-digital transformation. A large and growing library of downloadable apps helps to automate processes, saving time and improving workforce productivity. For example, single touch, cloud-connected apps allow users to scan directly to or from popular cloud-based repositories like Dropbox™ and Google Drive™

and scan to/print from Microsoft® Office 365®, transform paper documents to searchable PDFs right at the device or any other of the virtually unlimited options for hard-copy-to-digital document integration with proprietary and third-party document management systems like Microsoft SharePoint® and Xerox® DocuShare®.

* Xerox® AltaLink® devices only



Gateway to New Possibilities

Multifunction printers built on Xerox® ConnectKey® Technology are more than machines. They are workplace assistants and the centerpiece of a workplace transformation and productivity ecosystem combining all the technologies, capabilities and extensibility you need to let your work — and work teams — flow.

EASY, APP-BASED FUNCTIONALITY

ConnectKey Technology brings an entirely new level of flexibility, efficiency and possibility to your workforce with both its native apps and those available through the Xerox App Gallery.

Native apps simplify print, scan and copy functions as well as provide access to contact lists and frequently used locations, while apps available through the App Gallery allow users to download serverless apps like Connect 2.0 for Dropbox™ and Connect 2.0 for Microsoft® Office 365® directly from the user interface.

With Xerox App Gallery and Personalized Application Builder (PAB)*, Xerox partners can offer even more sophisticated levels of customization to automate your unique workflow requirements.

It all adds up to unlimited opportunities to streamline processes and improve productivity.



CLOUD CONNECTED

In addition to the extreme productivity you'll gain from ConnectKey and its mobile apps, our Xerox Extensible Interface Platform® (an open architecture software platform available on all ConnectKey Technology-enabled devices from entry level printers to large office multifunction printers) allows our partners and independent software developers to offer sophisticated solutions for document management, workflow automation, security and accounting.

With Xerox Extensible Interface Platform, your ConnectKey Technology-enabled printer or multifunction printer can adapt to the way you work with comprehensive, custom productivity-enhancing solutions for document management, accounting, mobile printing and user access controls.

Feature Focus

XEROX® EASY TRANSLATOR SERVICE

This service brings possibilities to life by allowing MFP users to scan a document and immediately receive a translated print and/or email notification. Documents or images can also be sent to the service from a PC, any iOS or Android™ device. It's just one example of the advanced capabilities and services available with Xerox® ConnectKey® Technology.

Find out more at www.xeroxtranslates.com.

* For Xerox channel partner customers. Xerox Direct sales customers should contact their sales executive for information on the Xerox® MFP Workflow App Customization Program.

Xerox® Devices Built on Xerox® ConnectKey® Technology

You'll work better, faster and smarter with a consistent user experience, mobile and cloud connectivity, easy automation, benchmark security and access to a growing library of apps to expand functionality and boost productivity.

COLOR LETTER/A4 DEVICES



Xerox® VersaLink®
C400 Color Printer



Xerox® VersaLink C500
Color Printer



Xerox® VersaLink
C600 Color Printer



Xerox® VersaLink
C405 Color
Multifunction Printer



Xerox® VersaLink C505
Color Multifunction
Printer



Xerox® VersaLink
C605 Color
Multifunction Printer

BLACK-AND-WHITE LETTER/A4 DEVICES



Xerox® VersaLink
B400 Printer



Xerox® VersaLink
B600 Printer



Xerox® VersaLink
B610 Printer



Xerox® VersaLink
B405 Multifunction
Printer



Xerox® VersaLink
B605 Multifunction
Printer



Xerox® VersaLink
B615 Multifunction
Printer

COLOR TABLOID/A3 DEVICES



Xerox® VersaLink
C7000 Color
Printer



Xerox® VersaLink
C8000 Color
Printer



Xerox® VersaLink
C9000 Color
Printer



Xerox® VersaLink
C7020/C7025/
C7030 Color
Multifunction
Printer



Xerox® AltaLink
C8030/C8035/
C8045/C8055/
C8070 Color
Multifunction
Printer

BLACK-AND-WHITE TABLOID/A3 DEVICES



Xerox® VersaLink
B7025/B7030/
B7035 Multifunction
Printer



Xerox® AltaLink
B8045/8055/8065/
8075/8090
Multifunction Printer

To learn more about Xerox® ConnectKey Technology, go to www.connectkey.com.

Security Guide

Xerox® AltaLink® B8145/B8155/B8170 Multifunction Printer

Xerox® AltaLink® C8130/C8135/C8145/C8155/C8170 Color Multifunction Printer



2020 Xerox Corporation. All rights reserved. Xerox®, CentreWare®, AltaLink®, Xerox Extensible Interface Platform® are trademarks of Xerox Corporation in the United States and/or other countries. BR# 28402

Other company trademarks are also acknowledged.

Document Version: 1.0 (January 2020).

Copyright protection claimed includes all forms and matters of copyrightable material and information now allowed by statutory or judicial law or hereinafter granted including without limitation, material generated from the software programs which are displayed on the screen, such as icons, screen displays, looks, etc.

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions

Contents

1. Introduction	1-1
Purpose	1-1
Target Audience	1-1
Disclaimer	1-1
2. Product Description	2-2
Physical Components	2-2
Architecture	2-3
User Interface	2-3
Scanner	2-3
Marking Engine	2-3
Controller	2-4
Controller External Interfaces	2-4
Front/Rear Panel USB (Type A) port(s)	2-4
10/100/1000 MB Ethernet TIA-568 Network Connector	2-4
Rear USB (Type B) Target Port	2-4
Optional Equipment.....	2-5
RJ-11 Analog Fax and Telephone	2-5
Wireless Network Connector.....	2-5
Bluetooth® MicroAdapter	2-5
Near Field Communications (NFC) Reader	2-5
SMART CARD – CAC/PIV	2-5
Foreign Product Interface.....	2-5
3. User Data Protection.....	3-1
User Data Protection While Within Product	3-1
Encryption	3-1
Private Key Management.....	3-1
Job Data Removal available on standard SSD configuration	3-1
Media Sanitization (Image Overwrite) available with optional HDD configuration	3-1
Overwriting Immediate Image Overwrite available with optional HDD configuration.....	3-1
On-Demand Image Overwrite available with optional HDD configuration	3-2
User Data in Transit	3-2
Inbound User Data (Print Job Submission).....	3-2

Email Signing and Encryption using S/MIME.....	3-2
Scanning to Network Repository, Email, Fax Server (Outbound User Data)	3-3
Scanning to User Local USB Storage Product (Outbound User Data).....	3-3
Add on Apps – Cloud, Google, DropBox, and others (Outbound User Data).....	3-4
4. Network Security	4-5
TCP/IP Ports and Services	4-5
Listening Services (inbound ports).....	4-6
Network Encryption	4-7
IPsec	4-7
Wireless 802.11 Wi-Fi Protected Access (WPA)	4-7
TLS.....	4-8
SNMPv3	4-8
Public Key Infrastructure (PKI).....	4-9
Device Certificates	4-9
Trusted Certificates	4-10
Minimum Key length.....	4-10
Network Access Control.....	4-11
802.1x.....	4-11
Cisco Identity Services Engine (ISE)	4-11
Contextual Endpoint Connection Management	4-12
FIPS140-2 Compliance Validation	4-12
Additional Network Security Controls.....	4-13
IP Filtering	4-13
Personal Identifiable Information (PII).....	4-13
5. Device Security: BIOS, Firmware, OS, Runtime, and Operational Security Controls	5-1
Pre-Boot Security	5-1
BIOS.....	5-1
Embedded Encryption	5-1
Boot Process Security	5-1
Trusted Boot.....	5-1
Firmware Integrity	5-2
Runtime Security	5-2
Operational Security.....	5-2
Firmware Restrictions	5-2
Event Monitoring and Logging	5-3

Configuration Watchdog.....	5-3
Audit Log	5-3
Security Information Event Management (SIEM) Support.....	5-4
Operational Security.....	5-4
Service Technician (CSE) Access Restriction	5-4
Additional Service Details	5-4
Cloning	5-4
Backup and Restore.....	5-5
EIP Applications	5-5
6. Configuration and Security Policy Management Solutions.....	6-1
7. Identification, Authentication, and Authorization.....	7-1
Authentication	7-1
Local Authentication.....	7-1
Network Authentication.....	7-1
Smart Card Authentication (CAC, PIV, SIPR, etc.).....	7-1
Convenience Authentication	7-1
Local Authentication.....	7-1
Password Policy.....	7-2
Network Authentication	7-2
Smart Card Authentication	7-2
Convenience Authentication	7-3
Xerox Workplace Cloud https://www.xerox.com/	7-3
Pharos print management solutions https://pharos.com/	7-3
YSoft SafeQ https://www.ysoft.com/en.....	7-3
Authorization (Role-Based Access Controls).....	7-3
Remote Access	7-3
Local Access	7-3
8. Additional Information and Resources	8-1
Security @ Xerox®	8-1
Responses to Known Vulnerabilities.....	8-1
Additional Resources	8-1
9. Appendix A: Product Security Profiles	9-2

AltaLink® B8145/B8155/B8170 & C8130/C8135/C8145/C8155/C8170.....	9-2
Physical Overview	9-2
Security Related Interfaces	9-3
Controller Non-Volatile Storage	9-3
Controller Volatile Memory	9-4
Marking Engine Non-Volatile Storage	9-4
Marking Engine Volatile Memory	9-4
10. Appendix B: Security Events	10-1
Xerox AltaLink Security Events	10-1

1. Introduction

Purpose

The purpose of this document is to disclose information for the AltaLink® multifunction devices (hereinafter called as “the product” or “the system”) with respect to product security. Product Security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a network environment, and how the product may be accessed both locally and remotely. The purpose of this document is to inform Xerox customers of the design, functions, and features of the product with respect to Information Assurance. This document does not provide tutorial level information about security, connectivity, or the product’s features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics.

Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

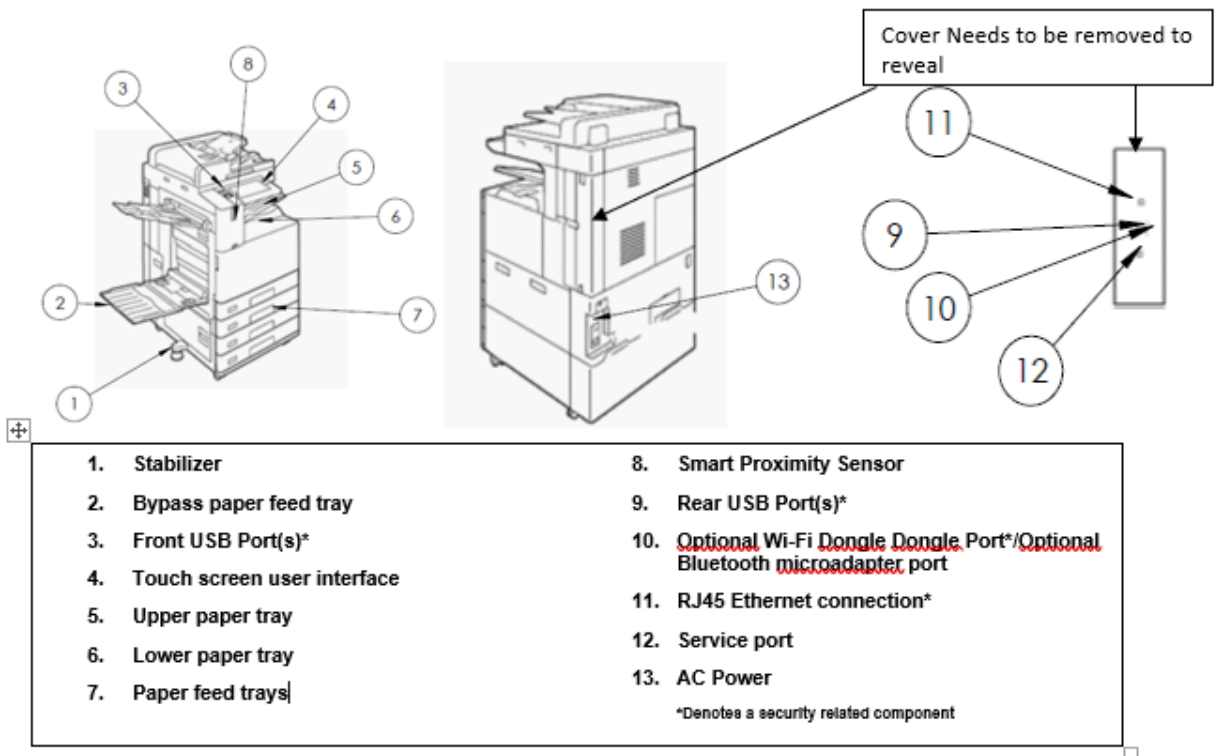
Disclaimer

The content of this document is provided for information purposes only. Performance of the products referenced herein is exclusively subject to the applicable Xerox Corporation terms and conditions of sale and/or lease. Nothing stated in this document constitutes the establishment of any additional agreement or binding obligations between Xerox Corporation and any third party.

2. Product Description

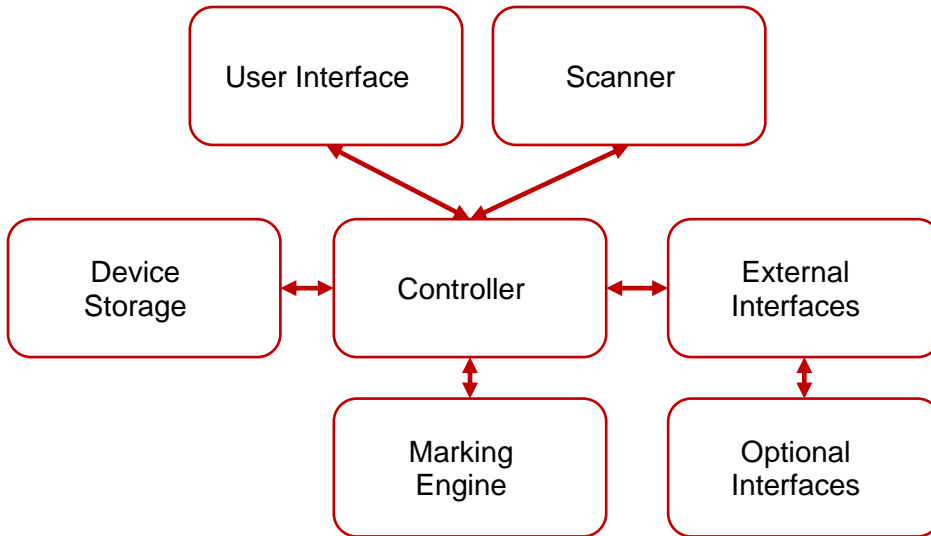
PHYSICAL COMPONENTS

Xerox® AltaLink® B8145/B8155/B8170 (Mono MFP) and C8130/C8135/C8145/C8155/C8170 (Color MFP) are very similar and consist of an input document handler and scanner, marking engine, controller, and user interface. A typical configuration is depicted below. Please note that options including finishers, paper trays, document handlers, etc. may vary configuration, however, they are not relevant to security and are not discussed.



ARCHITECTURE

AltaLink® products share a common architecture which is depicted below. The following sections describe components in detail.



USER INTERFACE

The user interface detects soft and hard button actuations and provides text and graphical prompts to the user. The user interface is sometimes referred to as the Graphical User Interface (GUI) or Local UI (LUI) to distinguish it from the remote web server interface (WebUI).

The user interface allows users to access product services and functions. Users with administrative privileges can manage the product configuration settings. User permissions are configurable through Role-Based Access Control (RBAC) policies, described in section 7 Identification, Authentication, and Authorization

SCANNER

The scanner converts documents from hardcopy to electronic data. A document handler moves originals into a position to be scanned. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images.

MARKING ENGINE

The Marking Engine performs copy/print paper feeding and transport, image marking, fusing, and document finishing. The marking engine is comprised of paper supply trays and feeders, paper transport, LED scanner, xerographics, and paper output and finishing. The marking engine is only accessible to the Controller via inter-chip communication with no other access and does not store user data.

CONTROLLER

The controller manages document processing using proprietary hardware and algorithms to process documents into high-quality electronic and/or printed reproductions. Documents may be temporarily buffered in RAM during processing. Standard models are equipped with a Solid State Disk (SSD). Optional magnetic Hard Disk Drive (HDD) is also available. For model specific details please see Appendix A: Product Security Profiles.

In addition to managing document processing the controller manages all network functions and services. Details can be found in section Network Security.

The controller handles all I/O communications with connected products. The following section provides a description of each interface. Please note that not all interfaces are supported on all models; details about each model can be found in Appendix A: Product Security Profiles.

Controller External Interfaces

FRONT/REAR PANEL USB (TYPE A) PORT(S)

One or more USB ports may be located on the front of the product, near the user interface. Front USB ports may be enabled or disabled by a system administrator. The front USB port supports the following:

- Walk-up users may insert a USB thumb drive to store or retrieve documents for scanning and/or printing from a FAT formatted USB device. The controller will only allow reading/writing of a limited set of known document types (such as, PDF, PNG, JPEG, TIFF, etc.). Other file types including binary executables are not supported.

Note: Features that use the USB ports (such as Scan To USB) can be disabled independently.

- Connection of optional equipment such as Bluetooth or CAC readers.
- Firmware updates may be submitted through the USB ports. Note that the product must be configured to allow local firmware updates, or the update will not be processed.

10/100/1000 MB ETHERNET TIA-568 NETWORK CONNECTOR

This is a standard Ethernet network connector and conforms to IEEE Ethernet 802.3 standards.

REAR USB (TYPE B) TARGET PORT

A USB type B port located on the controller board at the rear of the product. This port supports the following:

- USB target connector used for printing

Note: This port is used for service Diagnostics and cannot be disabled by a system administrator.

Optional Equipment

RJ-11 ANALOG FAX AND TELEPHONE

The embedded FAX service uses the installed embedded fax card to send and receive images over the telephone interface. The FAX card plugs into a custom interface slot on the controller. The fax telephone lines are connected directly to the Fax Card via RJ-11 connectors and it uses T.30 Fax Modem protocol and will not accept data or voice communication. All remaining fax-specific features are implemented in software on the controller.

WIRELESS NETWORK CONNECTOR

AltaLink® products accept an optional wireless kit that can be installed in the rear USB port.

BLUETOOTH® MICROADAPTER

AltaLink® products accept an optional Bluetooth MicroAdapter that can be installed in the rear USB port to support iBeacon for AirPrint Discovery.

When enabled and configured, iBeacon enables the Xerox® AltaLink® product to advertise basic printer discovery information, including a routable IP address, via the Bluetooth Low Energy Beacon. iBeacon functionality can be disabled using the embedded web server of the product.

NEAR FIELD COMMUNICATIONS (NFC) READER

AltaLink® products come standard with an NFC Chip built into the front panel. This is read only from an NFC client. The data exchanged is not encrypted and may include information including system network status, IP address and product location. NFC functionality can be disabled using the embedded web server of the product. NFC functionality requires a software plugin that can be obtained from Xerox sales and support.

Information shared over NFC includes: IPv4 Address, IPv6 Address, MAC Address, UUID (a unique identifier on the NFC client), and Fully qualified domain name

SMART CARD – CAC/PIV

AltaLink® products support a variety of smart cards that can be used to login to the machine. Please contact Xerox Support for a list of supported cards and card readers.

FOREIGN PRODUCT INTERFACE

This port is used to connect optional equipment to control access to the machine. A typical application is a coin-operated product where a user must deposit money to enable the machine to print. The information available via the Foreign Product Interface is limited to optically-isolated pulses that can be used to count impressions marked on hardcopy sheets. No user data is transmitted to or from this interface.

3. User Data Protection

Xerox printers and multifunction products receive, process, and may optionally store user data from several sources including as local print, scan, fax, or copy jobs or mobile and cloud applications, etc. Xerox products protect user data being processed by employing strong encryption. The standard configuration is sold with SSD.

User Data Protection While Within Product

This section describes security controls that protect user data while it is resident within the product. For a description of security controls that protect data in transit please refer to the following section that discusses data in transit; also, the Network Security section of this document.

ENCRYPTION

All user data being processed or stored to the product is encrypted by default. Encryption cannot be disabled on this family of products.

PRIVATE KEY MANAGEMENT

Any private key on the system is managed in compliance with NIST Special Publication 800-57 *Recommendation for Key Management*. This includes keying material in transition and at rest. An onboard TPM module (v2.0) compliant with ISO/IEC 11889 is used in support of private key management.

JOB DATA REMOVAL AVAILABLE ON STANDARD SSD CONFIGURATION

The Job Data Removal feature is provided to allow security conscious customers the facility to remove all residual image data from the Network Controller, the image system and, if installed, the Embedded Classic Fax card memory. Job Data Removal is being introduced to provide customers with SSD devices the ability to clean up the disk by purging job data (no overwrite) using the same interface as ODIO available with HDD configuration.

MEDIA SANITIZATION (IMAGE OVERWRITE) AVAILABLE WITH OPTIONAL HDD CONFIGURATION

AltaLink® products equipped with magnetic hard disk drives are compliant with NIST Special Publication 800-88 Rev1: *Guidelines for Media Sanitization*. User data is securely erased using a the algorithm as described in the following link:

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf>

OVERWRITING IMMEDIATE IMAGE OVERWRITE AVAILABLE WITH OPTIONAL HDD CONFIGURATION

When enabled, Immediate Image Overwrite (IIO) will overwrite any temporary files that were created on the magnetic hard disk that may contain user data. The feature provides continuous automatic overwrite of sensitive data with minimal impact to performance, robust error reporting, and logging via the Audit Log.

ON-DEMAND IMAGE OVERWRITE AVAILABLE WITH OPTIONAL HDD CONFIGURATION

Complementing the Immediate Image Overwrite is On-Demand Overwrite (ODIO). While IIO overwrites individual files, ODIO overwrites entire partitions. The ODIO feature can be invoked at any time and optionally may be scheduled to run automatically. When enabled, Immediate Image Overwrite (IIO) will overwrite and remove any remnants and temporary files of all print, copy, scan, and fax jobs from the image disk as soon as the job finishes processing. The feature provides continuous automatic overwrite of sensitive data with minimal impact to performance, robust error reporting, and logging via the Audit Log.

User Data in Transit

This section focuses on the protection of user data (print/scan/other jobs) in transit as they are submitted to the product for processing and/or are sent from the product to other systems. Additional protections are also discussed in the Network Security section of this document.

INBOUND USER DATA (PRINT JOB SUBMISSION)

In addition to supporting network level encryption including IPsec and WPA, Xerox products also support encryption of print job data at the time of submission. This can be used to securely transmit print jobs over unencrypted connections or to enhance existing network level security controls.

Encrypted Transport	Description
IPPS (TLS)	Submit print jobs via Secure Internet Printing Protocol. This protocol is based on HTTP and utilizes the TLS suite to encrypt data.
HTTPS (TLS)	Securely submit a print job directly to product via the built-in web server.
Xerox Print Stream Encryption	The Xerox Global Print Driver® supports document encryption for any print jobs to enabled products. Simply configure Document Encryption to On in the Advanced tab of the print driver at print time.

EMAIL SIGNING AND ENCRYPTION USING S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) provides Authentication, Message integrity, Non-repudiation, and encryption of email.

		AltaLink® Multifunction
		B8145, B8155, B8170, C8030, C8135, C8145, C8155, C8170
Email S/MIME		
	Versions	v3
	Digest	SHA1, SHA256, SHA384, SHA512
	Encryption	AES128, AES192, AES256

SCANNING TO NETWORK REPOSITORY, EMAIL, FAX SERVER (OUTBOUND USER DATA)

AltaLink® multifunction products support scanning of hardcopy documents to external network locations including file repositories and email and facsimile services. In addition to supporting network level encryption including IPsec, Xerox products support the following.

Protocol	Encryption	Description
HTTP	N/A	Unencrypted HTTP protocol.
HTTPS (TLS)	TLS	HTTP encrypted by TLS
FTP	N/A	Unencrypted FTP
SFTP (SSH)	SSH	FTP encrypted by SSH.
SMBv3	Yes	Encryption may be enabled on a Windows share
SMBv2	N/A	Unencrypted SMB
SMBv1	N/A	(Not used as a transport protocol. Used for network discovery only)
SMTP (email)	S/MIME	The product uses SMTP to transmit data to the email server. Email authentication, encryption, and signing are supported. Please refer to the Network Security section of this document for details.

SCANNING TO USER LOCAL USB STORAGE PRODUCT (OUTBOUND USER DATA)

Scan data is transferred directly to the user's USB product. Filesystem encryption of user products are not supported.

AltaLink® Multifunction		
B8145, B8155, B8170		
C8130, C8135, C8145, C8155, C8170		
Local Data Encryption		AES-256
Federal Information Protection Standard 140-2		Yes
Media Sanitization NIST 800-171 (Image Overwrite)		Models with magnetic HDD. See Appendix A: Product Security Profiles
Print Submission		
	IPPS (TLS)	Supported
	HTTPS (TLS)	Supported
	Xerox Print Stream Encryption	Supported
Scan to Repository Server		
	HTTPS (TLS)	1.0, 1.1, 1.2
	SFTP (SSH)	SSH-2
	SMB (unencrypted)	v1, v2, v3

	SMB (with share encryption enabled)	V3
	HTTP (unencrypted)	Supported
	FTP (unencrypted)	Supported
Scan to Fax Server		
	HTTPS (TLS)	1.0, 1.1.1, 1.2
	SFTP (SSH)	SSH-2
	SMB (unencrypted)	v1, v2, v3
	SMB (with share encryption enabled)	V3
	S/MIME	Supported
	HTTP (unencrypted)	Supported
	FTP (unencrypted)	Supported
	SMTP (unencrypted)	Supported
Scan to Email		
	S/MIME	Supported
	SMTP (unencrypted)	Supported
	TLS (Start TLS)	Supported

ADD ON APPS – CLOUD, GOOGLE, DROPBOX, AND OTHERS (OUTBOUND USER DATA)

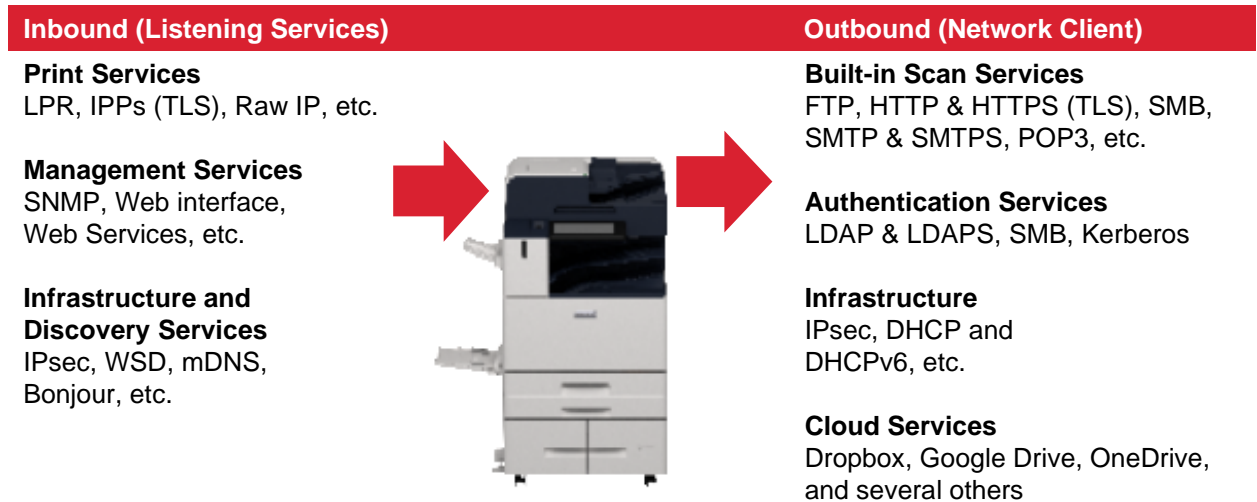
The Xerox App Gallery® contains several additional applications that extend the capabilities of Xerox products. Discussion of App security is beyond the scope of this document. Xerox Apps utilize the security framework provided by the third-party vendor. (For example, Microsoft O365 or Google Apps would utilize Microsoft and Google’s security mechanisms respectively). Please consult documentation for individual Apps and third-party security for details.

4. Network Security

Xerox products are designed to offer a high degree of security and flexibility in almost any network environment. This section describes several aspects of the product related to network security.

TCP/IP Ports and Services

Xerox devices are robust, offering support for a wide array of services and protocols. The devices are capable of hosting services as well as acting as a client for others. The diagram below presents a high-level overview of inbound communications (from other hosts on the network into listening services on the device) and outbound connections initiated by the device (acting as a client to external network services).



LISTENING SERVICES (INBOUND PORTS)

The following table summarizes all potentially open ports on the product. These ports can be enabled/disabled within the product configuration. Some ports can be configured to different value for some features/protocols.

Port	Type	Service Name
80 or 443	TCP	HTTP including: Web User Interface Web Services for Products (WSD) WebDAV
68	UDP	DHC ACK Response to DHCP
88	UDP	Kerberos
110	TCP	POP3
139	TCP	NETBIOS
161	TCP	SNMP
162	TCP	SNMP Trap
137	UDP	NETBIOS (Name Service)
138	UDP	NETBIOS (Datagram Service)
161	UDP	SNMP
427	TCP/UDP	SLP
443	TCP	HTTPS – HTTP over TLS, IPPS
445	TCP	SMB
500 & 4500	TCP/UDP	IPsec
515	TCP	LPR
631	TCP	IPP
3702	TCP/UDP	WSD (Discovery)
4000	TCP	ThinPrint
5353	TCP/UDP	mDNS
5354	TCP	mDNS Responder IPC
9100	TCP	Raw IP (also known as JetDirect, AppSocket or PDL-datastream)
5909-5999	TCP	Remote Access to local display panel. Port is randomly selected and communications encrypted with TLS 1.2
51333	TCP	Device File Distribution downloads
53202	TCP	WSD Transfer
53303	TCP	WSD Print
53404	TCP	WSD Scan

Network Encryption

IPSEC

Internet Protocol Security (IPsec) is a network security protocol capable of providing encryption and authentication at the packet level. AltaLink® products support IPsec for both IPv4 and IPv6 protocols.

		AltaLink® Multifunction
		B8145, B8155, B8170, C8130, C8135, C8145, C8155, C8170
IPsec		
	Supported IP Versions	IPv4, IPv6
	Key exchange authentication method	Preshared Key & digital signature authentication (device authentication certificate, server validation certificate)
	Transport Mode	Transport & Tunnel mode
	Security Protocol	ESP & AH
	ESP Encryption Method	AES, Null
	ESP Authentication Methods	SHA1, SHA256, None

WIRELESS 802.11 WI-FI PROTECTED ACCESS (WPA)

Products equipped with WiFi support WPA2 Personal, WPA2 Enterprise, and Mixed Mode compliant with IEEE 802.11i. The wireless network adapters used in Xerox products are certified by the Wi-Fi Alliance.

		AltaLink® Multifunction
		B8145, B8155, B8170, C8130, C8135, C8145, C8155, C8170
Wi-Fi (802.11)		
	No Encryption	Supported
	WEP	RC4
	WPA2 Personal (PSK)	CCMP (AES), TKIP, TKIP+CCMP (AES)
	WPA2 Enterprise	CCMP (AES), TKIP, TKIP+CCMP (AES) PEAPv0 MS-CHAPv2 EAP-TLS EAP-TTLS/PAP EAP-TTLS/MS-CHAPv2 EAP-TTLS/EAP-TLS

	BSSID Roaming Restriction	Supported
--	---------------------------	-----------

TLS

AltaLink® products support the latest version, TLS 1.2 and the default setting is TLS1.0.

AltaLink® Multifunction
B8145, B8155, B8170,
C8030, C8135, C8145, C8155, C8170

TLS Versions Supported		
	Product Web Interface	1.2, 1.1, 1.0
	Product Web Services	1.2, 1.1, 1.0
	Product IPPS printing	1.2, 1.1, 1.0
	Remote control	1.2

SNMPV3

SNMPv3 is the current standard version of SNMP defined by the Internet Engineering Task Force (IETF). It provides three important security features:

Message integrity to ensure that a packet has not been tampered with in transit

Authentication to verify that the message is from a valid source

Encryption of packets to prevent unauthorized access

AltaLink® Multifunction
B8145, B8155, B8170, C8030, C8135, C8145, C8155, C8170

SNMPv3		
	Digest	SHA1, MD5
	Encryption	DES, AES128

Public Key Infrastructure (PKI)

Digital certificates are a key component of public key infrastructure. A digital certificate contains information about the identity of an entity, the certificate authority that issued the certificate, and its associated public and private key pair. The certificate's private key is used to generate digital signatures, and the public key is used to validate those digital signatures. For entities to validate a digital signature, the certificate and its public key are shared freely. Trust is established by validating the certificate path, which contains the certificate authorities that issued the certificate.

DEVICE CERTIFICATES

AltaLink® products support both CA signed and self-signed device certificates. The device certificates support a bit length of up to 4096 bits.

AltaLink® products require a device certificate. The MFP will use the device certificate as its identity. The MFP EWS certificate is an example of a device certificate. The device certificate must be issued by a certificate authority (CA) trusted by the device.

The Xerox device certificate, which is the default device certificate installed on the MFP, is issued by the Xerox Root CA embedded in the MFP firmware. The Xerox device certificate details are configurable and can be recreated as needed by the device administrator.

The MFP can be configured to use any installed CA signed certificate as its device certificate. To install a CA signed certificate, the device administrator can generate and download a Certificate Signing Request (CSR) from the MFP, have the CSR signed by an Enterprise CA or 3rd Party CA, and then import the CA signed certificate into the MFP. Alternatively, this process can be completed off-box and a CA signed certificate in PKCS #12 format can be imported into the MFP.

AltaLink® Multifunction		
B8145, B8155, B8170, C8030, C8135, C8145, C8155, C8170		
Device Certificates		
	Certificate Length	Up to 4096 (for RSA certificates)
	Default Device Certificate	ECDSA P-384
	Supported Hashes	SHA256
	Product Web Server	Supported
	IPPS Printing	Supported
	802.1X Client	Supported
	IPsec	Supported
	SFTP	Supported

TRUSTED CERTIFICATES

Public Root and Intermediate Root Certificate Authority (CA) certificates may be imported to the product's certificate store to establish trust with external products and services. The following categories are supported:

- A Root CA certificate is a certificate with authority to sign other certificates. These certificates usually are self-signed certificates that come from another product or service that you want to trust.
- An Intermediate CA certificate is a certificate that links a certificate to a Trusted Root CA Certificate in certain network environments.
- Peer Device certificates are certificates that are installed on the printer for solution-specific uses.

		AltaLink® Multifunction
		B8145, B8155, B8170, C8030, C8135, C8145, C8155, C8170
Trusted Certificates (CA & Peer device)		
	Minimum Length RSA Restriction Options	None, 1024, 2048
	Maximum Length	4096
	Supported Hashes	SHA1/224/256/384/512
	IPsec	Supported
	LDAP	Supported
	Scanning (HTTPS/TLS)	Supported
	Scanning (SFTP/SSH)	Used for audit log transfer
	802.1X Client	Supported
	Email Signing	Supported
	Email Encryption	Supported
	Email (STARTLS)	Supported
	OCSP Signing	Supported

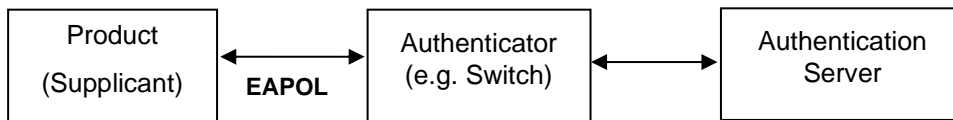
MINIMUM KEY LENGTH

An administrator can specify the minimum encryption key length required for certificates. If a user attempts to upload a certificate that contains a key that does not meet this requirement, a message appears. The message alerts the user that the certificate they are attempting to upload does not meet the key length requirement.

Network Access Control

802.1X

In 802.1X authentication, when the product is connected to the LAN port of Authenticator such as the switch as shown below, the Authentication Server authenticates the product, and the Authenticator controls access of the LAN port according to the authentication result. The product starts authentication processing at startup when the startup settings for 802.1X authentication are enabled.



AltaLink® Multifunction		
B8145, B8155, B8170, C8030, C8135, C8145, C8155, C8170		
Network Access Control		
	802.1x	Supported
	Authentication Methods	EAP-MD5, PEAPv0/EAP MSCHAPv2, EAP-MSCHAPv2, EAP-TLS

CISCO IDENTITY SERVICES ENGINE (ISE)

Cisco ISE is an intelligent security policy enforcement platform that mitigates security risks by providing a complete view of which users and what products are being connected across the entire network infrastructure. It also provides control over what users can access your network and where they can go. Cisco's ISE includes over 200 Xerox product profiles that are ready for security policy enablement. This allows ISE to automatically detect Xerox products in your network. Xerox products are organized in Cisco ISE under product families, such as AltaLink® products, enabling Cisco ISE to automatically detect and profile new Xerox products from the day they are released. Customers who use Cisco ISE find that including Xerox products in their security policies is simpler and requires minimal effort.

Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. ISE collects various attributes for each network endpoint to build an endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of product profiles. These profiles include a wide range of product types, including tablets, smartphones, cameras, desktop operating systems (for example, Windows®, Mac OS® X, Linux® and others), and workgroup systems such as Xerox printers and MFPs.

Once classified, endpoints can be authorized to the network and granted access based on their profile signature. For example, guests to your network will have different level of access to printers and other end points in your network. As an example, you and your employees can get full printer access when accessing the network from a corporate workstation but be granted limited printer access when accessing the network from your personal Apple® iPhone®.

Cisco ISE allows you to deploy the following controls and monitoring of Xerox products: Automatically provision and grant network access rights to printers and MFPs to prevent inappropriate access (including automatically tracking new printing products connecting to the network):

- Block non-printers from connecting on ports assigned to printers
- Prevent impersonation (aka spoofing) of a printer/MFP
- Automatically prevent connection of non-approved print products
- Smart rules-based policies to govern user interaction with network printing products

Provide simplified implementation of security policies for printers and MFPs by:

- Providing real time policy violation alerts and logging
- Enforcing network segmentation policy
- Isolating the printing products to prevent general access to printers and MFPs in restricted areas

Automated access to policy enforcement

- Provide extensive reporting of printing product network activity

AltaLink® Multifunction		
B8145, B8155, B8170, C8030, C8135, C8145, C8155, C8170		
Network Access Control		
	Cisco ISE	Supported

CONTEXTUAL ENDPOINT CONNECTION MANAGEMENT

Traditionally network connection management has been limited to managing endpoints by IP address and use of VLANs and firewalls. This is effective, but highly complex to manage for every endpoint on a network. Managing, maintaining, and reviewing the ACLs (and the necessary change management and audit processes to support them) quickly become prohibitively expensive. It also lacks the ability to manage endpoints contextually.

Connectivity of AltaLink® devices can be fully managed contextually by Cisco TrustSec. TrustSec uses Security Group Tags (SGT) that are associated with an endpoint's user, device, and location attributes. SG-ACLs can also block unwanted traffic so that malicious reconnaissance activities and even remote exploitation from malware can be effectively prevented.

FIPS140-2 COMPLIANCE VALIDATION

When enabled, the product will validate its current configuration to identify cryptographic modules in use. Modules which are not FIPS 140-2 (Level 1) compliant will be reported.

AltaLink® products include FIPS compliant algorithms of SNMPv3 and Kerberos, however, an exception can be approved to run these in non-FIPS compliant mode when configured for non-FIPS algorithms.

Additional Network Security Controls

IP FILTERING

The devices contain a static host-based firewall that provides the ability to prevent unauthorized network access based on IP address and/or port number. Filtering rules can be set by the SA using the WebUI. An authorized SA can create rules to (Accept/Reject/Drop) for ALL or a range of IP addresses. In addition to specifying IP addresses to filter, an authorized SA can enable/disable all traffic over a specified transport layer port.

PERSONAL IDENTIFIABLE INFORMATION (PII)

Personal Identifiable Information (PII) can be entered or stored into the device through several means: address book, scan templates, device description, display device information, audit logs, and engineering logs. The PII is encrypted on the device and it is not readable outside of the operation of the device. The Admin controls the ability of users to enter data, and controls the accessibility of logs, or th may be resident.

5. Device Security: BIOS, Firmware, OS, Runtime, and Operational Security Controls

AltaLink® products have robust security features that are designed to protect the system from a wide range of threats. Below is a summary of some of the key security controls.

Pre-Boot Security

BIOS

The BIOS used in AltaLink® products is embedded and cannot be accessed directly. Unlike devices such as desktop and laptop computers that have a BIOS that can be accessed via a keystroke on startup, the BIOS of AltaLink® products is not accessible.

Many devices can be cleared to factory defaults (including passwords and security settings) by depressing a reset button using a paperclip or similar method. For security reasons, AltaLink® products do not offer such a method to clear or reset the BIOS. (Note that configuration settings may be reset to factory defaults by an authorized administrator, however, this does not impact BIOS settings).

BIOS updates can be securely applied by device firmware updates. Firmware is protected from tampering by use of digital signatures (discussed later in this section).

The BIOS is designed to fail secure. An integrity check is performed immediately when power is applied. If verification is successful, the system proceeds with OS kernel boot. If the integrity check fails, the system will fail secure.

EMBEDDED ENCRYPTION

AES encryption is used to protect the system, user data, and configuration (including security settings) from being retrieved or modified. Each device uses its own unique key that is securely generated. Encryption is enabled by default. Media encryption and sanitization are discussed in Section 3 User Data Protection.

Boot Process Security

TRUSTED BOOT

Xerox® AltaLink® MFPs utilize a Trusted Boot process to enable a secure boot utilizing Intel's Boot Guard and the Unified EFI Forum/Microsoft specified (UEFI) BIOS approach to ensure a verified Chain of Trust is utilized to perform the MFP boot process. This process establishes a root of trust extending from the Intel processor to the UEFI and continuing to the Boot Manager and the Xerox Firmware. The startup process verifies that the installation software/firmware has not been altered, giving the customer assurance that the code has not been altered or replaced.

FIRMWARE INTEGRITY

Unlike open operating systems such as servers and user workstations in which software may be installed by users, Xerox products are based on embedded systems and the contents are managed by Xerox. The only means of modifying the contents of a device is by applying a firmware update package.

Firmware updates use a special format and each firmware update are encrypted and digitally signed to protect the integrity of the contents. Firmware that is corrupt or has been illicitly modified will be rejected. This security control cannot be disabled. AltaLink® products include a built-in firmware software validation. This is a file integrity monitor that compares the security hashes of currently installed firmware to a secured whitelist that was installed when the signed firmware was installed.

Runtime Security

Each AltaLink® device comes with McAfee Embedded Control built-in and enabled by default and cannot be disabled. McAfee Embedded Control is used to protect a variety of endpoints that range from wearable devices to critical systems controlling electrical generation.

Executable control prevents unauthorized code from executing. Xerox has defined a whitelist of executable programs; software that is not on the secure whitelist is not allowed to execute. McAfee cannot be disabled on AltaLink® products; it is always enabled.

Memory control monitors memory and running processes. If unauthorized code is injected into a running process, it is detected and prevented.

When an anomaly is detected it is logged to the device audit log and optional alerts are immediately sent via email. Events are also reportable through CentreWare® Web or Xerox Device Manager, and McAfee® ePolicy Orchestrator® (ePO).

Operational Security

FIRMWARE RESTRICTIONS

The list below describes supported firmware delivery methods and applicable access controls.

Local Firmware Upgrade via USB port:

Xerox service technicians can update product firmware using a USB port and specially configured USB thumb drive.

Network Firmware Update:

Product system administrators can update product firmware using the Embedded Web Server. The ability to apply a firmware update is restricted to roles with system administrator or Xerox service permissions. Firmware updates can be disabled by a system administrator.

Xerox Remote Services Firmware Update:

Xerox Remote Services can update product firmware securely over the internet using HTTPS. This feature can be disabled, scheduled, and includes optional email alerts for system administrators.

The programs stored in the Flash ROM listed below are downloadable from external sources.

Controller

Marking Engine

Scanner

Document Feeder

Finisher (Option for processing printed paper. No description on Finisher is provided in this document because user's image data will not be stored in it.)

High capacity feeder (No description on High capacity feeder is provided in this document because user's image data will not be stored in it.)

High capacity stacker (No description on high capacity stacker is provided in this document because user's image data will not be stored in it.)

Interface Module (No description on interface module is provided in this document because user's image data will not be stored in it.)

The downloading function can be disabled by a system administrator from the local UI or the Embedded Web Server.

For additional information on Firmware updates and various upgrade methods supported, please see the System Administrator Guide.

Event Monitoring and Logging

CONFIGURATION WATCHDOG

The Atlantis 2.1 firmware allows Administrators to configure the periodic monitoring of up to thirty-four security-related settings. If, during a check, a monitored security setting is discovered to have been changed, the system will automatically reset it. In the case that remediation is unsuccessful, an email alert is generated, and the event is captured in the Audit Log (see below for information on the Audit Log). For a list of the security settings covered, please see the System Administrator Guide.

AUDIT LOG

The Audit Log feature records security-related events. The Audit Log contains the following information:

Field	Description
Index	A unique value that identifies the event
Date	The date that the event happened in mm/dd/yy format
Time	The time that the event happened in hh:mm:ss format
ID	The type of event. The number corresponds to a unique description
Description	An abbreviated description of the type of event
Additional Details	Columns 6–10 list other information about the event, such as: Identity: User Name, Job Name, Computer Name, Printer Name, Folder Name, or Accounting Account ID display when Network Accounting is enabled. Completion Status Image Overwrite Status: The status of overwrites completed on each job. Immediate Image must be enabled.

AltaLink® products currently support over a hundred unique events. A maximum of 15,000 events can be stored on the device. When the Audit Log reaches 13,500 entries (90% “full”), an email alert will be sent. When it reaches 28,500 events, the device will send another message stating there have been 15,000 events since the last alert. The device will keep alerting at 15,000 event intervals. When the number of events exceeds 15,000, audit log events will be deleted in order of timestamp, and then new events will be recorded. The audit log can be exported at any time by a user with administrative privileges. Note that as a security precaution, audit log settings and data can only be accessed via HTTPS and Audit Log can't be disabled on this version of AltaLink® products.

SECURITY INFORMATION EVENT MANAGEMENT (SIEM) SUPPORT

Xerox® AltaLink® supports the ability to directly connect to industry leading security and event management (SIEM) systems. Once configured, Xerox® AltaLink® MFPs send security information, along with the event severity, to the SIEM system for processing and reporting. The Atlantis 2.1 firmware supports connection to McAfee Enterprise Security Manager and LogRhythm Threat Detection. By supporting multiple SIEM solutions, Xerox® AltaLink® MFPs offer our customers the flexibility of choosing the SIEM system that best fits their environment.

Operational Security

SERVICE TECHNICIAN (CSE) ACCESS RESTRICTION

The CSE (Customer Service Engineer) account allows a Xerox Technicians to access the MFP's diagnostics and maintenance routines. The CSE role has only 'guest privileges' to the other user interfaces including the Local and WebUI. However, CSE access to these other interfaces can be restrict if needed.

ADDITIONAL SERVICE DETAILS

Xerox products are serviced by a tool referred to as the Portable Service Workstation (PWS). Only Xerox authorized service technicians are granted access to the PWS. Customer documents or files cannot be accessed during a diagnostic session, nor are network servers accessible through this port. If a network connection is required while servicing a Xerox device, service technicians will remove the device from any connected networks. The technician will then connect directly to the device using an Ethernet cable, creating a physically secure and isolated network during service operations.

CLONING

Certain system settings can be captured (copied) in a clone file that may be installed on other AltaLink systems. Clone files are encrypted and this AltaLink MFP does not support installing older clone files created on other Atlantis 1.0 and 1.5 devices. Access to both creating and installing a clone file can be restricted using role-based access controls. Clone files can only be created through the Embedded Web Server or via USB at the Local UI. Clone files can be installed through the following methods: Embedded Web Server, USB at the Local UI, Web service, submission as a print job, or file distribution.

BACKUP AND RESTORE

Like cloning, backup & restore, can capture (copy) certain system and device specific settings in a backup file. This file may be reapplied to the same device at any time. This backup can be stored at the device or exported, and the exported file is encrypted.

EIP APPLICATIONS

Xerox products can offer additional functionality through the Xerox Extensible Interface Platform® (EIP). Third party vendors can create Apps that extend the functionality of a product. Xerox signs EIP applications that are developed by Xerox or Xerox partners. Products can be configured to prevent installation of unauthorized EIP applications. Discussion of individual EIP application security is beyond the scope of this document. EIP applications utilize the security framework provided by the Third-party vendor and the EIP configuration of the product. Please consult documentation for individual EIP application as provided by the Third-party vendor for security details.

6. Configuration and Security Policy Management Solutions

Xerox Device Manager and Xerox® CentreWare® Web (available as a free download) centrally manage Xerox Devices. Additionally, AltaLink® products come with McAfee built in and can be managed with McAfee ePO™ providing an enhanced security posture supporting proactive monitoring, threat detection, and remediation capabilities. For details please visit Xerox.com or speak with a Xerox representative.

7. Identification, Authentication, and Authorization

AltaLink® products offer a range of authentication and authorization options to support various environments.

Single Factor authentication is supported locally on the product or via external network authentication servers (e.g., LDAP, Kerberos, ADS). Multi Factor authentication is supported by addition of card reader hardware. (Where ease of access is desired, open access and simple user identification modes also exist, however these are not recommended for secure environments.)

In all modes, product administrator accounts always require authentication. This cannot be disabled.

A flexible RBAC (Role-Based Access Control) security model enables granular control to assign user permissions. Once a user has been authenticated, the product grants (or denies) user permissions based upon the role(s) they have been assigned to. Pre-defined roles that may be used or custom roles may be created as desired.

Authentication

Xerox® AltaLink® devices support the following authentication mode:

Local Authentication

Network Authentication

Smart Card Authentication (CAC, PIV, SIPR, etc.)

Convenience Authentication

LOCAL AUTHENTICATION

The local user database stores user credential information. The printer uses this information for local authentication and authorization, and for Xerox Standard Accounting. When you configure local authentication, the printer checks the credentials that a user provides against the information in the user database. When you configure local authorization, the printer checks the user database to determine which features the user is allowed access. Each device has a unique default administrator password which should be changed as soon as possible along with enabling recommended security features to secure the system.

Note: User names and passwords stored in the user database are not transmitted over the network and passwords are encrypted.

PASSWORD POLICY

The following password attributes can be configured:

Password Policy	
Minimum Length	1
Maximum Length	63
Default Minimum	4
Password cannot contain User Name	Supported
Password complexity options (in addition to alphabetic characters)	Can be set to require a number, an upper case character, lower case character and a special character

Admin password can be set using any character within the printable Unicode and the AltaLink default administrator password meets the 2020 California Password Law (SB-327). This law states that each 'internet-connectable' device must have a unique password by default.

All newly sold Xerox devices will have the default administrator password be the serial number of the device. It is recommended the customer change this new default administrator password, as soon as possible, to a strong password that the customer can use and recall.

NETWORK AUTHENTICATION

When configured for network authentication, user credentials are validated by a remote authentication server.

Network Authentication Providers	
Kerberos (Microsoft Active Directory)	Supported
Kerberos (MIT)	Supported
SMB NTLM Versions Supported	NTLMv2
LDAP Versions Supported	Version 3 (including TLS 1.2)

SMART CARD AUTHENTICATION

Smart Card authentication is considered very secure due to the nature of the Smart Card architecture and potential levels of encryption of data on the card itself. It provides two-factor security: 1) a PIN is required to unlock the smart card and 2) the user's smart card credential is authenticated over the network using Kerberos PKINIT authentication.

Smart Card Authentication requires card reader hardware. Please contact Xerox Support for a list of supported cards and card readers.

Smart Cards	
Common Access Card (CAC)	Supported
PIV/ PIV II	Supported
Gemalto MD	Supported
SIPR	Supported

Support for the SIPR network is provided using a Smart Card authentication solution created by 90meter under contract for Xerox. Details regarding 90meter can be found online here: <https://www.90meter.com/>

CONVENIENCE AUTHENTICATION

Convenience authentication offloads authentication to a third-party solution which may offer more or less security than native security implementations. Users swipe a pre-programmed identification card or key fob to access the device.

For example, employees may be issued key fobs for access to facilities. Convenience mode may be configured to allow an employee to authenticate using their fob or require the fob in a multi-factor manner. The level of security provided is dependent upon the chosen implementation.

Some examples of third-party convenience authentication providers include:

Xerox Workplace Cloud <https://www.xerox.com/>

Pharos print management solutions <https://pharos.com/>

YSoft SafeQ <https://www.ysoft.com/en>

Contact your Xerox sales representative for details and other options.

Authorization (Role-Based Access Controls)

AltaLink® products offer granular control of user permissions. Users can be assigned to pre-defined roles or customers may design highly flexible custom permissions. A user must be authenticated before being authorized to use the services of the product. Authorization ACLs (Access Control Lists) are stored in the local user database. Authorization privileges (referred to as permissions) can be assigned on a per user or group basis.

Please note that Xerox products are designed to be customizable and support various workflows as well as security needs. User permissions include security-related permissions and non-security related workflow permissions (e.g., walkup user options, copy, scan, plex, etc.). Only security-related permissions are discussed here.

REMOTE ACCESS

Without RBAC permissions defined basic information such as model, serial number, and software version can be viewed by unauthenticated users. This can be disabled by restricting access to the device website pages for non-logged-in users.

By default, users are allowed to view basic status and support related information, however they are restricted from accessing device configuration settings. Permission to view this information can be disallowed.

LOCAL ACCESS

Without RBAC permissions defined basic information such as model, serial number, software version, IP address, and host name can be viewed without authentication. This can be disabled by disallowing access to device settings for unauthenticated users.

By default, users are allowed to access the local interface, however, they are restricted from accessing device configuration settings. Roles can be configured to allow granular access to applications, services, and tools. Users can be also restricted from accessing the local interface completely.

8. Additional Information and Resources

Security @ Xerox®

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see <https://www.xerox.com/security>.

Responses to Known Vulnerabilities

Xerox has created a document which details the Xerox Vulnerability Management and Disclosure Policy used in discovery and remediation of vulnerabilities in Xerox software and hardware. It can be downloaded from this page: <https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html>

Additional Resources

Below are additional resources.

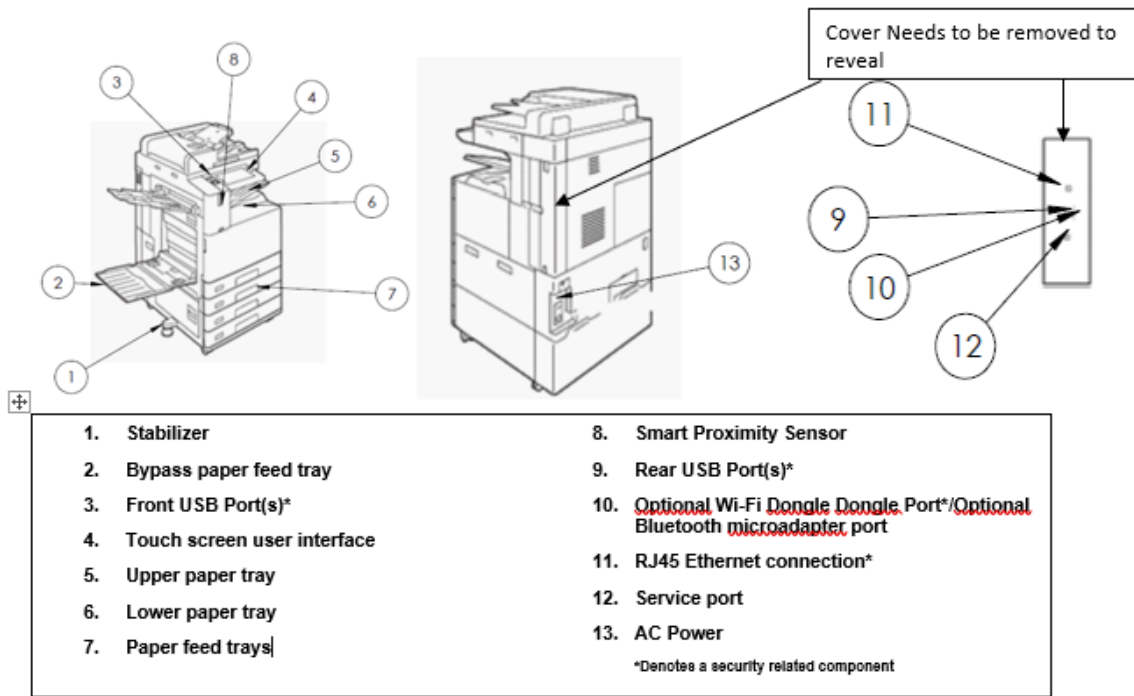
Security Resource	URL
Frequently Asked Security Questions	https://www.xerox.com/en-us/information-security/frequently-asked-questions
Common Criteria Certified Products	https://security.business.xerox.com/en-us/documents/common-criteria/
Current Software Release Quick Lookup Table	https://www.xerox.com/security
Bulletins, Advisories, and Security Updates	https://www.xerox.com/security
Security News Archive	https://security.business.xerox.com/en-us/news/

9. Appendix A: Product Security Profiles

This appendix describes specific details of each AltaLink® product.

AltaLink® B8145/B8155/B8170 & C8130/C8135/C8145/C8155/C8170

PHYSICAL OVERVIEW



SECURITY RELATED INTERFACES

Security Related Interfaces	
Ethernet	10/100/1000 MB Ethernet interface.
Optional Wi-Fi Dongle	Supports optional 802.11 Dongle.
Optional Bluetooth MicroAdapter	Supports optional iBeacon support for AirPrint Discovery through Bluetooth Low Energy Beacons.
Rear USB 3.0 (Type B)	USB target connector used for printing. Note: This port can be disabled completely by a system administrator.
Front & Rear USB2.0 (Type A) port(s)	Users may insert a USB thumb drive to print from or store scanned files to. (Physical security of this information is the responsibility of the user or operator.) Note that features that leverage USB ports (such as Scan To USB) can be disabled independently based on services. Firmware upgrades may be applied using this port. Connection of optional equipment such as NFC or CAC readers. Note: This port can be disabled completely by a system administrator.

CONTROLLER NON-VOLATILE STORAGE

Model	Size	Type	Use	User Data	How to Clear	Non-Volatile
B8170, B8155, B8145, C8130, C8135, C8145, C8155, C8170	120 GB or higher	SSD*	Contains User Data (e.g., Print, Scan, Fax) and Configuration Settings. This data is encrypted and Encryption is always-on	Yes	Factory Reset	Yes
B8170, B8155, B8145, C8130, C8135, C8145, C8155, C8170	320 GB	HDD**	Contains User Data (e.g., Print, Scan, Fax) and Configuration Settings. This data is encrypted and Encryption is always-on	Yes	Factory Reset	Yes

*SSD: Solid State Drive, is a Standard Configuration **HDD: Magnetic Hard Disk Drive, is a purchasable option

CONTROLLER VOLATILE MEMORY

Model	Size	Type	Use	User Data	How to Clear	Non-Volatile
B8170, B8155, B8145, C8130, C8135, C8145, C8155	4 GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes
C8170	8 GB	DDR3 DRAM	Executable code, Printer control data, temporary storage of job data	Yes	Power off system	Yes

Additional Information: The controller operating system memory manager allocates memory dynamically between OS, running processes, and temporary data which includes jobs in process. When a job is complete, the memory pages in use are freed and reallocated as required by the OS.

MARKING ENGINE NON-VOLATILE STORAGE

The marking engine does not contain any non-volatile storage.

MARKING ENGINE VOLATILE MEMORY

The marking engine volatile memory does not store or process user data.

10. Appendix B: Security Events

Xerox AltaLink Security Events

ID	Event	Description
1	System Startup	Device Name Device Serial Number
2	System Shutdown	Device Name Device Serial Number
3	Standard ODIO Started	Device Name Device Serial Number
4	Standard ODIO Complete	Device Name Device Serial Number Overwrite Status
5	Print Job	Job Name User Name Source Service Name Completion Status IIO Status Accounting User ID Accounting Account ID
6	Network Scan Job	Job Name User Name Completion Status IIO status Accounting User ID Accounting Account ID Total Number Net Destination Net Destination
7	Server Fax Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Total Fax Recipient Phone Numbers Fax Recipient Phone Numbers Net Destination
8	iFax	Job Name User Name Completion Status IIO Status

		Accounting User ID Accounting Account ID Total Number of SMTP Recipients SMTP Recipients
9	Email Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Encryption On or Off Total Number of SMTP Recipients SMTP Recipients
10	Audit Log Disabled	Device Name Device Serial Number
11	Audit Log Enabled	Device Name Device Serial Number
12	Copy Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID
13	Embedded Fax	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Total Fax Recipient Phone Numbers Fax Recipient Phone Numbers
14	LAN Fax Job	Job Name User Name Completion Status IIO Status Accounting User ID Accounting Account ID Total Fax Recipient Phone Numbers Fax Recipient Phone Numbers
16	Full ODIO Started	Device Name Device Serial Number
17	Full ODIO Complete	Device Name Device Serial Number Overwrite Status
20	Scan to Mailbox Job	Job Name or Directory Name

		User Name Completion Status IIO Status
21	Delete File/Directory	Job Name or Directory Name User Name Completion Status IIO Status
23	Scan to Home	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
24	Scan to Home Job	Job Name or Directory Name User Name Completion Status (Normal/Error) IIO Status Accounting User ID Name Accounting Account ID Name Total Number Net Destination Net Destination
25	Copy Store Job	Job Name or Directory Name User Name Completion Status (Normal/Error) IIO Status
26	PagePack Login	Device Name Device Serial Number Completion Status: Success (if Passcode is okay) Failed (if Passcode is not okay) Locked Out (if max attempts exceed 5) Time Remaining: Hrs (Remaining for next attempt) Min (Remaining for next attempt)
27	Postscript Passwords	Device Name Device Serial Number Startup Mode or System Params Password or Start Job Password
29	Network User Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
30	SA Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
31	User Login	User Name Device Name

		Device Serial Number Completion Status (Success/Failed)
32	Service Login	Service Name Device Name Device Serial Number Completion Status (Success/Failed)
33	Audit Log Download	User Name Device Name Device Serial Number Destination (WebUI, USB drive) Completion Status (Success/Failed)
34	IIO Feature Status	User Name Device Name Device Serial Number IIO Status (Enabled/Disabled)
35	SA Pin Changed	User Name Device Name Device Serial Number Completion Status
36	Audit Log Saved	User Name Device Name Device Serial Number Completion Status
38	X509 Certificate	User Name Device Name Device Serial Number Completion Status (Created/Uploaded/Downloaded)
39	IP Sec	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled/Terminated)
40	SNMPv3	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled/Terminated)
41	IP Filtering Rules	User Name Device Name Device Serial Number Completion Status (Rule Added/Rule Edited/Rule Deleted)
42	Network Authentication	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled)

43	Device Clock	User Name Device Name Device Serial Number Completion Status (Time Zone Changed/Date/Time Changed/Time Format Changed/Date Format Changed)
44	SW Upgrade	User Name Device Name Device Serial Number Completion Status (Success/Failed)
45	Cloning	User Name Device Name Device Serial Number Completion Status
46	Scan Metadata Validation	Device Name Device Serial Number Completion Status (Success/Failed)
47	Xerox Secure Access	Device Name Device Serial Number Completion status (Configured/Enabled/Disabled)
48	Service Login Copy Mode	Service Name Device Name Device Serial Number Completion Status (Success/Failed)
49	Smartcard (CAC/PIV) Access	User Name (if valid Card and Password are entered) Device Name Device Serial Number Completion Status (Success/Failed)
50	Process Terminated	Device Name Device Serial Number Process Name Termination Reason
51	ODIO Scheduled	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled) ODIO Schedule Mode Configured ODIO Schedule Frequency Configured ODIO Schedule Day of Week Configured ODIO Schedule Day of Month Configured
53	CPSR Backup	File Name User Name Completion Status (Normal/Error) IIO Status
54	CPSR Restore	File Name

		User Name Completion Status (Normal/Error) IIO Status
55	SA Tools Access Admin	Device Serial Number Completion Status (Locked/Unlocked)
57	Session Timer Logout	Device Name Device Serial Number Interface (WebUI, LUI, CAC) User Name (who was logged out) Session IP (if available)
58	Session Timer Interval Change	Device Name Device Serial Number Interface (WebUI, LUI, CAC) (Timer affected by change) User Name (who made this change) Session IP (if available) Completion Status (Success/Failed)
59	Feature Access Control	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured) Interface (WebUI, LUI, CAC, SNMP) Session IP Address (if available)
60	Device Clock NTP	Device Name Device Serial Number Enable/Disable/Config NTP NTP Server IP Address/Hostname Server Port Completion Status (Success/Failed)
61	Grant/Revoke Admin Rights	Device Name Device Serial Number User Name (of target user) Grant or Revoke (the admin right) Completion Status (Success/Failed)
62	Smartcard (CAC/PIV)	User Name Device Name Device Serial Number Card type (SIPR Token, CAC/PIV) Completion Status (Success/Failed)
63	IPv6	User Name Device Name Device Serial Number Completion Status (Success/Failed)
64	802.1x	User Name Device Name Device Serial Number Completion Status (Success/Failed)
65	Abnormal System Termination	Device Name Device Serial Number

66	Local Authentication	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
67	Web User Interface Authentication	User Name Device Name Device Serial Number Authentication Method Enabled (Network/Local)
68	FIPS Mode	User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configure)
69	Xerox Secure Access Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
70	Print from USB	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
71	USB Port Enable/Disable	User Name Device Name Device Serial Number USB Port ID Completion Status (Enabled/Disabled)
72	Scan to USB	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
73	System Log Download	Username Device Name File Names Downloaded Destination (IP address or USB device) Completion Status (Success/Failed)
74	Scan to USB Job	Job Name User Name Completion Status IIO Status Accounting User ID Name Accounting Account ID Name
75	Remote UI Feature	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
76	Remote UI Session	User Name Device Name Device Serial Number Completion Status (Initiated/Terminated) Remote Client IP Address

77	Remote Scan Feature (Driver)	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
78	Remote Scan Job Submitted (Driver)	User Name (at client if available) IP Address of Submitting Client Device Name Device Serial Number Job Name (if accepted) Completion Status (Accept/Reject/Request)
79	Scan to Web Service Job Remote Scan Job Completed (Driver)	Job name User Name Accounting User ID Name Accounting Account ID Name Completion Status (Destination)
80	SMTP Connection Encryption	User Name Device name Device Serial Number Completion Status (Enabled for STARTLS/ Enabled for STARTLS if available/ Enabled for TLS/Disabled/Configured)
81	Email Domain Filtering Rule	User Name Device Name Device Serial Number Completion Status (Feature Enabled/Feature Disabled/Rule Added/Rule Deleted)
82	Software Self Test Started	Device Name Device Serial Number
83	Software Self Test Complete	Device Name Device Serial Number Completion Status (Success/Failed/Cancelled)
84	McAfee Security State	User Name Device Name Device Serial Number Security Mode (Enhanced Security/Integrity Control) Completion Status (Enabled/Disabled/Pending)
85	McAfee Security Event	Device Name Device Serial Number Type (Read/Modify/Execute/Deluge) McAfee Message Text
87	McAfee Agent	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
88	Digital Certificate Import Failure	Device Name Device Serial Number Email Address of Requestor (if available) Failure Reason (Invalid Address/Invalid Certificate/Invalid Signature)

89	User Name Add/Delete	User Name (Managing User Names) Device Name Device Serial Number User Name Added or Deleted Completion Status (Created/Deleted)
90	User Name Password Change	User Name (Managing Passwords) Device Name Device Serial Number User Name Affected Completion Status (Password Modified)
91	eFax Job Secure Print Passcode	User Name (Managing Passcodes) Device Name Device Serial Number Completion Status (Passcode Created/Changed)
92	Scan2Mailbox Folder Password Change	User Name (Managing Passwords) Device Name Device Serial Number Folder Name Completion Status (Password was Changed)
93	eFax Mailbox Passcode	User Name (Managing Passcodes) Device Name Device Serial Number Completion Status (Passcode Created/Changed)
94	FTP/SFTP Filing Passive Mode	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
95	eFax Forwarding Rule	User Name Device Name Device Serial Number Fax Line 1 or 2 (if applicable) Completion Status (Rule Edit/Rule Enabled/Rule Disabled)
96	EIP Weblets Allow Install	User Name Device Name Device Serial Number Completion Status (Enable Installation/Block Installation)
97	EIP Weblets Install	User Name Device Name Device Serial Number Weblet Name Action (Install/Delete) Completion (Success/Fail)
98	EIP Weblets Enable	User Name Device Name Device Serial Number Weblet Name Completion Status (Enable/Disable)
99	Network Connectivity	User Name Device Name

		Device Serial Number Completion Status (Enable Wireless/Disable Wireless/ Configure Wireless/Enable Wired/Disable Wired/ Configure Wired/Enable WiFi Direct/Disable WiFi Direct/Configure WiFi Direct)
100	Address Book Permissions	User Name Machine Name Machine serial number Completion Status (SA Only/Open Access Enabled WebUI)/ (SA Only/Open Access Enabled LocalUI)
101	Address Book Export	User Name Machine Name Machine Serial Number
102	SW Upgrade	User Name Device Name Device Serial Number Completion Status (Enable Installation/Disable Installation)
103	Supplies Plan Activation	Device Name Device Serial Number Completion Status Success (if Passcode is okay) Failed (if Passcode is not okay) Locked out (if Max Attempts Exceed 5) Time Remaining Hrs (remaining for next attempt) Min (remaining for next attempt)
104	Plan Conversion	Device Name Device Serial Number Completion Status Success (if Passcode is okay) Failed (if Passcode is not okay) Locked out (if Max Attempts Exceed 5) Time Remaining Hrs (remaining for next attempt) Min (remaining for next attempt)
105	IPv4	User Name Device Name Device Serial Number Completion Status (Enabled Wireless/Disabled Wireless/ Configured Wireless/Enabled Wired/Disabled Wired/ Configured Wired)
106	SA PIN Reset	Device Serial Number Completion Status (Success/Failed)
107	Convenience Authentication Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
108	Convenience Authentication	User Name Device Name Device Serial Number Completion Status

		(Enabled/Disabled/Configured)
109	eFax Passcode Length	User Name (Managing Passcodes) Device Name Device Serial Number Completion Status (Passcode Length Changed)
110	Custom Authentication Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)
111	Custom Authentication	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
112	Billing Impression Mode	User Name Device Name Device Serial Number Mode Set to (A4 Mode/A3 Mode) Completion Status (Success/Failed)
114	Device Cloning	User Name Device Name Device Serial Number Completion Status (Enable for Encrypted Files Only/Disable)
115	Save for Reprint Job	Job Name User Name Print from USB/Print from URL Completion Status
116	WebUI Access Configure	Device Name Device Serial Number Completion Status (Standard Access/Open Access/Restricted)
117	System Log Push to Xerox	Username if Authenticated Server Destination URL Log Identifier String (Filename) Completion Status (Success/Failed)
119	Scan to WebDAV Job	Job Name User Name Completion Status IIO status Accounting User ID Name Accounting Account ID Name WebDAV Destination
123	Near Field Communication	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
124	Invalid Login Attempt Lockout	Device Name Device Serial Number Interface (WebUI, Local UI) Session IP Address (if available)

125	Protocol Audit Log Enable/Disable	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
126	Display Device Information Configure	User Name Device Name Device Serial Number Completion Status (Configured)
127	Invalid Login Lockout Expires	Device Name Device Serial Number Interface (WebUI) Session IP Address (if available) Count of Invalid Attempts: xx attempts, where xx = the number of attempts
128	Erase Customer Data	Device Serial Number Erase Customer Data Device Serial Number Completion Status (Success/Failed)
129	Audit Log SFTP Scheduled Configure	User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured)
130	Audit Log SFTP Transfer	User Name Device Name Device Serial Number Destination Server Completion Status (File Transmitted)
131	Remote Software Download	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
132	AirPrint & Mopria Scanning	User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured)
133	AirPrint & Mopria Scan Job Submitted	Job Name (if accepted) User Name (if available) IP Address of Submitting Client Device Name Device Serial Number Completion Status (Accept/Reject Request)
134	AirPrint & Mopria Scan Job Completed	Job Name User Name (if available) Completion Status
136	Remote Services NVM Write	Device Name Device Serial Completion Status (Success/Fail)
137	Remote Services FIK Install	Device Name Device Serial

		Completion Status (Success/Fail) User-readable names for the features being installed
138	Remote Services Data Push	Device Name Device Serial Completion Status (Success/Fail)
139	Remote Services	User Name, Device Name Device Serial Status (Enabled/Disabled)
140	Restore	User Name Device Name Device Serial Number Completion Status (Enable/Disable)
141	Backup-Restore File Downloaded	File Name User Name Interface (WebUI) IP Address of the Destination (if applicable) Completion Status (Success/Failed)
142	Backup-Restore Restore Installed	File Name User Name Device Name Device IP address Interface (WebUI) Completion Status (Success/Failed)
143	Google Cloud Services	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
144	User or Group Role Assignment	User Name Device Name Device Serial Number User or Group Name (Assigned) Role Name Action (Added/Removed)
145	User Permission Role	User Name Device Name Device Serial Number Role Name Completion Status (Created/Deleted/Configured)
146	Admin Password Policy Configure	User Name Device Name Device Serial Number
147	Local User Account Password Policy	User Name Device Name Device Serial Number
148	Restricted Admin Login	User Name Device Name Device Serial Number Completion Status (Success/Failed)

149	Grant/Revoke Restricted Admin Rights	User Name (of user making the change) Device Name Device Serial Number User Name (of target user) Action (Grant/Revoke)
150	Manual Session Logout	Device Name Device Serial Number Interface (WebUI, LUI, CAC) User Name (who was logged out) Session IP (if available)
151	IPP	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
152	HTTP Proxy Server	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
153	Remote Services Software Download	Device Name Device Serial Number File Name
154	Restricted Admin Permission Role	User Name Device Name Device Serial Number Restricted Admin Role Name Completion Status (Created/Deleted/Configured)
155	EIP Weblet Installation Security Policy	User Name Device Name Device Serial Number Policy (Allow Installation of Encrypted Weblets/Allow Installation of Both Encrypted and Unencrypted Weblets)
156	Lockdown and Remediate Security	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
157	Lockdown Security Check Complete	User Name Device Name Device Serial Number Completion Status (Success/Failed)
158	Lockdown Remediation Complete	User Name Device Name Device Serial Number Completion Status (Success/Failed)
159	Send Engineering Logs on Data Push	User Name (if available) Device Name Device Serial Number Current Setting (Enabled/Disabled)

160	Allow the Print Submission of Clone Files	User Name (if available) Device Name Device Serial Number Completion Status (Enabled/Disabled)
161	Network Troubleshooting Start/Stop	User Name Device Name Device Serial Number Completion Status (Started/Stopped)
162	Network Troubleshooting Data Download	User Name File Name (of downloaded file) Device Name Device Serial Number Destination (IP Address) Completion Status (Success/Failed)
163	DNS-SD Text File Download	User Name File Name (of downloaded file) Device Name Device Serial Number Destination (IP address) Completion Status (Success/Failed)
164	1-Touch App Management	User Name Device Name Device Serial Number 1-Touch Application Display Name Action (Install/Un-install) Completion Status (Success/Failed)
165	SMB Browse	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
166	Job Data Removal Standard Started	Device Name Device Serial Number
167	Job Data Removal Standard Complete	Device Name Device Serial Number Completion Status (Success/Failed)
168	Job Data Removal Full Started	Device Name Device Serial Number
169	Job Data Removal Full Complete	Device Name Device Serial Number Completion Status (Success/Failed)
170	Scheduled Job Data Removal Configure	User Name Device Name Device Serial Number Completion Status (Enable/Disable/Configured)
171	Cross-Origin Resource Sharing (CORS)	User Name Device Name Device Serial Number Completion Status (Enable/Disable)

172	1-Touch App Export	User Name Device Name Device Serial Number Completion Status (Success/Failed)
173	Device File Distribution Trust Operations	User Name Device Name Device Serial Number Member Name Member Serial Number TC Lead Device Name TC Lead Serial Number Trust Operation (Grant/Revoke) Completion Status (Success/Failed)
174	Device File Distribution Feature	User Name Device Name Device Serial Number Trust Operation (Enable/Disable/Configure) Completion Status (Success/Failed)
175	Device File Distribution – Store File for Distribution	User Name Device Name Device Serial Number File type (SWUP/Clone/Add-On) File Name
176	Xerox Configuration Watchdog	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
177	Xerox Configuration Watchdog Check Complete	User Name (if available, SYSTEM, if executed as a scheduled event) Device Name Device Serial Number Completion Status (Success/Failed)
178	Xerox Configuration Watchdog Remediation Complete	User Name (if available, SYSTEM, if executed as a scheduled event) Device Name Device Serial Number Completion Status (Success/Failed)
179	ThinPrint Feature	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled/Configured)
180	Beaconing for iBeacon for AirPrint Discovery	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
181	Network Troubleshooting	User Name Device Name Device Serial Number Completion Status (Installed/Uninstalled)
182	POP3 Connection Encryption (TLS)	User Name Device Name

		Device Serial Number Completion Status (Enabled/Disabled/Configured)
183	FTP Browse	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled)
184	SFTP Browse	User Name Device Name Device Serial Number Completion Status (Configured/Enabled/Disabled)
189	Smart Proximity Sensor Sleep on Departure	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
190	Cloud Service	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
192	Scan to Cloud Job	Job Name User Name Cloud Service Completion Status IIO Status Accounting User ID Name Accounting Account ID Name
193	Xerox Workplace Cloud	User Name Device Name Device Serial Number Completion Status (Enabled/Disabled)
194	Scan to Save FTP and SFTP Credentials Policy	User Name Device Name Device Serial Number Completion Status (Never/Always/Prompt)
195	Card Reader	Device Name Device Serial Number Completion Status (Connected/Disconnected)
196	EIP Apps	User Name Device Name Device Serial Number App Name Action (Install/Delete) Completion Status (Success/Failed)
197	EIP Apps	User Name Device Name Device Serial Number App Name Action (Install/Delete) Completion Status (Enabled/Disabled)
204	Syslog Server	User Name

		Device Name Device Serial Number Server IPv4 Address (if available) Server IPv6 Address (if available) Completion Status (Configured/Enabled/Disabled)
205	TLS (Version and/or Hash)	User Name Device Name Device Serial Number Completion Status (Configured)

Xerox Resources:

Coordinate contract implementation, including designating associated Project Manager
The Account General Managers, Contract Manager, along with support from the Account Team, will be responsible to ensure efficient and effective management and administration of the contract.

Implementations will be project managed by the Client Manager and the Sales Manager for each location. There is an extended team of support resources that will be involved with each implementation and your Client Manager will facilitate this team and is responsible for:

- Communicating key information to the Project Team.
- Establishing and adhering to the schedule.
- Coordinating activities for all other Project Team members.
- Providing documentation, including weekly status reports and changes as required.
- Making Project Team members aware of all project details, issues and decisions.
- Obtaining project closure.

Account management for on-going contract monitoring, maintenance and communication Manager
Xerox understands and will comply.

Account Representative(s) dedicated to UC Locations Manager
Xerox understands and will comply. Please also refer to Section III, D.1.

To insure customer service satisfaction, Supplier is required to call customer 3 days after equipment installation and training. Customer shall be defined as a designated user for that location. For UC Locations with MFD/Printer Fleet Management Programs, Customer shall be defined as the designated contacts for those Programs Manager

Xerox understands and will comply.

Follow up will be completed by the assigned Xerox Client Manager supporting the install.

On-site sales representation on a regular basis to increase sales activity, assist in resolving problems, demonstrate new products, provide unlimited training and other customer services as required for the efficient operation of the program Manager

Xerox understands and will comply.

Coordinate all the order/installation process, inquiries regarding order status, and pricing concerns
Xerox understands and will comply. Assigned Xerox Client Manager will complete all of the above items.

Regular contact and/or meetings (frequency to be determined by each location, though no less than quarterly) between Supplier's account manager and UC Purchasing and/or MFD/Printer Fleet Management Program at each location to discuss issue resolution, performance activities and all related issues.

Xerox understands and will comply.

As part of our continuing engagement process, UC representatives and the Xerox account team will hold account review meetings on a regular basis, or as requested.

The main objective of these account reviews is to discuss operational and technical issues and performance against standards. Topics discussed may include: open issues and progress toward resolution, proposed /impending changes, status of special projects, optimization/future state review, any UC support requirements, UC management support and UC communication needs.

Monthly Operational Review Meetings

Xerox will schedule joint communication and status review meetings with UC's designated focal point as required. Topics typically discussed include:

- Customer support and communication requirements.
- Solution activity, metrics, and any analytics.
- Open issues and progress toward resolution.
- Recommendations for changes.

Quarterly Business Review

A formal management meeting will be held at a mutually agreed upon location and time. The primary purpose of this meeting is to discuss the services and their relationship to UC's strategic business goals. The meeting agenda will be mutually agreed upon, and may include the following topics:

- Review of the service level reports, trends, and overall services performance.
- Review of the progress of the resolution of previously discussed open issues.
- Services performance relative to strategic goals.

Semi Annual Executive Review

Xerox and UC's executives will hold a semi-annual executive review to discuss mutual objectives, customer business improvement opportunities and strategies. Topics may include:

- Annual performance review.
- Innovation proposals and opportunities.
- Major business and technology changes affecting services delivery or effectiveness.
- Maintain a customer service satisfaction level of 98% or better as evidenced by the results of regular customer survey's conducted by supplier.

Xerox understands and will comply.

Customer satisfaction and loyalty are Xerox's number one priority. For this reason, we consistently and proactively elicit customer feedback using a combination of relationship and event-based survey programs. We continuously monitor and polish these programs to ensure we understand the end to end customer experience signals retrieved from the relationship survey and utilize our event-based data to further diagnose deficiencies and drive improvements.

Xerox conducts 4 relationship surveys per year (one per quarter) with the goal of obtaining a response from the key decision makers in every account. We utilize a closed-loop management process to review survey results and establish action plans based on those results to ensure positive experiences and interactions with our customers.

Xerox tests, validates and ensures that we are meeting our customers' expectations based on honest feedback that we have obtained through measurement tools such as surveys. We ask for satisfaction feedback so that we can continue to make incremental process improvements that support our customers' business needs.

In addition, Xerox has expanded our standard proactive customer satisfaction system to include a very unique customer polling system called Sentinel TM. We designed the Sentinel system to facilitate gathering end-user customer feedback on a regular basis in order to systematically listen to all employees across a customer's enterprise.

With UC's permission, Sentinel will send a simple e-mail that prompts one of four responses: delete, send a comment, make a suggestion, or alert Xerox of a problem. Comments, suggestions and problems will "alert Xerox of an opportunity," automatically opening a dialog box that is completely viewable by

each customer from start to finish. With web-based Sentinel, concerns go straight from your company to Xerox. The system instantly notifies a Xerox Problem Solver, who personally owns the comment through a closed-loop resolution process.

The Sentinel “sense and respond” system is a proactive way for Xerox to receive and quickly respond to your feedback. We believe this system sets us apart from our competitors by creating a unique opportunity for our customers to share their thoughts—promoting interaction and collaboration that will strengthen our bottom-line relationships.

A designated contact for billing/invoicing questions and issues
Accounts are assigned to a specific biller and manager. All billing and invoice inquiries go to our Customer Care Center, where we have multiple resources available to respond to all billing and invoicing questions and issues.

Trade-In Equipment. University warrants that University has the right to transfer title to the Equipment University is trading in as part of an Order ("Trade-In Equipment"), and that the Trade-In Equipment is in good working order and has not been modified from its original configuration (other than by Xerox). Title and risk of loss to the Trade-In Equipment will pass to Xerox when Xerox removes the Trade-In Equipment from University's premises. University will maintain the Trade-In Equipment at its present site and in substantially the Trade-In Equipment's present condition until removed by Xerox. University will pay all accrued charges for the Trade-In Equipment, up to and including payment of the final principal payment number and all applicable maintenance, administrative, supply and finance charges until Xerox removes the Trade-In Equipment from the University's premises.

Upgrades. Xerox's Purchase and Maintenance as well as Xerox Lease offer allows the University to place additional equipment mainframe orders at the same quoted contract price throughout the 60-month master agreement term, provided each additional equipment placement remains installed for a minimum 60-month term. Xerox will also provide a separate price quote if the University desires to acquire additional equipment having an installation term less than 60-months. The equipment's features and performance can also be upgraded through the addition of a number of optional accessories. Accessory options included with the mainframe can be obtained at the contract quoted price. Any accessory ordered following the mainframe's installation will have the price readjusted based on the mainframe's remaining agreement term.

Please remember that the Xerox Purchase and Maintenance as well as Xerox Lease offering is based on a firm 60-month equipment installation term that can only be terminated due to fiscal year funds non-appropriation or an uncured performance failure. If the equipment is cancelled for the University's convenience and not replaced, or traded to a different unit, the University will be assessed a liquidated damages charge. In order to avoid this charge, Xerox recommends that the equipment either be: (a) exchanged with another University unit, or (b) moved to another University location and replaced with a unit that fits the end users current work requirements.



Time and Materials

Current Changes

65191

Time and Materials Price List

Current Changes

Time and Materials Price List

Xerox Form Number	Issue Date	Price List Name	Reason Changed
Sale Range 65191	02/15/17	Time and Materials Price List	ADVANCE Pricing Effective 04/01/18



Time and Materials **ADVANCED** Price List

Effective 04/01/18 (Supersedes 05/01/17)

1. **TIME:** Below are the labor rates charged for repair of equipment not covered by Basic Services. The rates are subject to change without notice. Charges do not include replacement parts used in repair. Replacement parts used in repair will be billed in addition to the labor charge. See item 2 on next page.

LABOR RATES FOR HIGH END PRODUCTS (NEW AND USED)			
DocuTech/Nuvera:	PP135, NP135, All Nuvera, 6100, 6115, 6135, 6155, 6180, HighLight Color 180/155/128, XDOD / DigiPath, SBMF, SBMF-1, SBMF-2, SFBM, SQFBM & DBSF		
High End System Printing:	MICR/Non-MICR, IPS, LPS, NPS; 4050, 4250, 4650, 4075, 4090, 4135, 4635, DP96, DP100, DP135, DP155, DP180, DP390, DP425DUP, DP425DUPU, DP500, DP500DUP, DP525DUP, DP525DUPU, DP525DUP1, DP525MX-MX1-MX2, CF495DUP, CF650DUP, CCF490, DP2K100, DP2K115, DP2K135, DP2K155, DP2K180, HLC128, HCL155, HCL180, HLCP128, HLCP155 & HLCP180, ESPRESSO, All CiPress, any and all DFEs that support these products.		
Production Color:	Fiery, Splash, Creo (Scites), DocuSP, DocuColor 2045/2060/6060/5352/5000/6060/7000/8000, C60/C70, X700s, X770s, & any and all iGEN models up through and including iGEN 5, 8250 and all DFEs that support these products.		
Early Production Color:	V180B, V180P, V3100, V80B, V80P, V2100, C75, J75, XC800/XC1000/ XC800P/XC1000P/XC1000i, XC550, XC560, XC570, and any all associated DFEs that support these products.		
Production Ink Jet:	Brenva HD, Rialto 900, Trivor 2400HD, All Xerox iPrint Products and any all associated DFEs that support these products.		
CALL CHARGE (INCLUDES FIRST 30 MINUTES OF LABOR)	LABOR RATES PER ADDITIONAL 15 MINUTES OR PORTION THEREOF (UNIT OF SERVICE)		
	REGULAR BUSINESS HOURS 8:00 AM TO 5:00 PM MONDAY - FRIDAY EXCEPT HOLIDAYS	PREMIUM BUSINESS HOURS (AS AVAILABLE IN LOCATION) 5:01 PM TO 7:59 AM MONDAY - FRIDAY AND ALL DAY SATURDAY EXCEPT HOLIDAYS	SUNDAY AND HOLIDAY BUSINESS HOURS (AS AVAILABLE IN LOCATION) ALL DAY NATIONAL HOLIDAYS AS OBSERVED BY XEROX
\$820.00	\$94.00	\$146.00	\$194.00

T&M service on PRINTERS not listed below are conducted by the Xerox Office Group. Please call 1-800-835-6100 for support.

LABOR RATES FOR PRINTERS & A4 MFPs PRODUCTS (NEW AND USED)			
Products: VersaLink B400, B405, C400, C405, C500, C505, C600, C605, 3330, 4150, 4250, 4260, 4600, 5550, 6510, 6700, 7760, 7800, CC20, CC118, CC123, CC128, CC133, CFFPMAPP, FFFPMAPP, IFFPMAPP, M118, WC15, WC123, WC128, WC133, WC3335/3345, WC3550, WC4118, WCM20, WC3335/3345, WC6400.			
CALL CHARGE (INCLUDES FIRST 30 MINUTES OF LABOR)	LABOR RATES PER ADDITIONAL 15 MINUTES OR PORTION THEREOF (UNIT OF SERVICE)		
	REGULAR BUSINESS HOURS 8:00 AM TO 5:00 PM MONDAY - FRIDAY EXCEPT HOLIDAYS	PREMIUM BUSINESS HOURS (AS AVAILABLE IN LOCATION) 5:01 PM TO 7:59 AM MONDAY - FRIDAY AND ALL DAY SATURDAY EXCEPT HOLIDAYS	SUNDAY AND HOLIDAY BUSINESS HOURS (AS AVAILABLE IN LOCATION) ALL DAY NATIONAL HOLIDAYS AS OBSERVED BY XEROX
\$314.00	\$72.00	\$123.00	\$152.00

LABOR RATES FOR FACSIMILE PRODUCTS (NEW AND USED)			
Products: DFC735, DFC745, DWC535, DWC545, DWC635, DWC645, DWC657, DWC665, DWC765, FC12, F110, F116, F2121, F2218, WCP555, WCP575, WCP580, WCP685, WCP785			
CALL CHARGE (INCLUDES FIRST 30 MINUTES OF LABOR)	LABOR RATES PER ADDITIONAL 15 MINUTES OR PORTION THEREOF (UNIT OF SERVICE)		
	REGULAR BUSINESS HOURS 8:00 AM TO 5:00 PM MONDAY - FRIDAY EXCEPT HOLIDAYS	PREMIUM BUSINESS HOURS (AS AVAILABLE IN LOCATION) 5:01 PM TO 7:59 AM MONDAY - FRIDAY AND ALL DAY SATURDAY EXCEPT HOLIDAYS	SUNDAY AND HOLIDAY BUSINESS HOURS (AS AVAILABLE IN LOCATION) ALL DAY NATIONAL HOLIDAYS AS OBSERVED BY XEROX
\$320.00	\$27.00	\$149.00	\$185.00



Time and Materials **ADVANCED** Price List

Effective 04/01/18 (Supersedes 05/01/17)

LABOR RATES For All Products NOT Previously Listed (includes Xerox Wide Format products)			
CALL CHARGE (INCLUDES FIRST 30 MINUTES OF LABOR)	LABOR RATES PER ADDITIONAL 15 MINUTES OR PORTION THEREOF (UNIT OF SERVICE)		
	REGULAR BUSINESS HOURS 8:00 AM TO 5:00 PM MONDAY - FRIDAY EXCEPT HOLIDAYS	PREMIUM BUSINESS HOURS (AS AVAILABLE IN LOCATION) 5:01 PM TO 7:59 AM MONDAY - FRIDAY AND ALL DAY SATURDAY EXCEPT HOLIDAYS	SUNDAY AND HOLIDAY BUSINESS HOURS (AS AVAILABLE IN LOCATION) ALL DAY NATIONAL HOLIDAYS AS OBSERVED BY XEROX
\$437.00	\$79.00	\$136.00	\$168.00

A. Service Call Charge: A Call Charge is assessed per machine service call. A Call Charge includes travel to the Customer site and up to 30 minutes of labor at that site.

B. Unit of Service: A unit of service is defined as 15 minutes of service or any portion thereof. A Call Charge includes two units of service (up to 30 minutes). Any additional units of service will be billed at the above labor rates.

2. MATERIALS:

Parts used in repair will be invoiced at the then current commercial list prices, which are subject to change without notice. Replacement parts may be recovered or reprocessed, at Xerox' option. All parts used in association with a service call are billable. Replaced parts become the property of Xerox at Xerox' option. Xerox will issue partial credit for selected replaced parts that Xerox deems repairable.

3. AFTER HOURS SERVICE FOR EQUIPMENT COVERED BY BASIC SERVICES:

For most equipment covered by Basic Services, for which service is requested after Xerox' standard business hours or any customer contracted for Extended Service Hours, the charge for both time (labor) and materials (parts) will be at a flat fee of **\$676.00** per call. The flat fee for the products identified above as "High End Products" is **\$820.00** per call. These fees are subject to change without notice. After Hours service is available in most areas as determined by Xerox local business practices.

Note: The after hours flat fee does not apply to the Xerox Wide Format products. The labor rates shown in item 1 above apply for these products.

4. TIME AND MATERIALS WARRANTY:

All labor is warranted for 30 calendar days from the date of service. All replacement parts are warranted for 30 calendar days from the time of installation on the machine.

5. REMOTE SERVICE SURCHARGE:

A. State of Alaska:

1. An additional 25% surcharge will be added to the labor charge for Time & Materials and After-Hours service repairs performed on products located in service Zones A, B and C.
2. Supplemental Zone C charges (applies to both FSMA and T&M):
 - a. Customer Service Engineer round trip transportation expenses from Juneau, Anchorage, or Fairbanks to machine location, if required, plus;
 - b. Customer Service Engineer food and lodging expenses, if required, plus;
 - c. Customer Service Engineer portal to portal charges, if required, or;
 - d. Zone surcharge.

3. ZONE DEFINITION

ZONE A Zone A is restricted to Customers within a geographic area within a 50 mile driving radius of those areas that currently have resident service coverage. These areas are Anchorage, Bethel, Fairbanks, Juneau, Kenai, Kodiak, Palmer and Soldotna.

Time and Materials **ADVANCED** Price List

Effective 04/01/18 (Supersedes 05/01/17)

- ZONE B Zone B locations are those areas accessible by road that are up to 50 miles beyond the Zone A limit. These include Glennallen, Delta Junction, Fort Greeley, Denali National Park, Healy, Seward, Talkeetna, and Whittier.
- ZONE C Zone C locations are all other areas of Alaska not accessible by road or more than 100 miles from Anchorage, Bethel, Fairbanks, Juneau, Kenai, Kodiak, Palmer and Soldotna. These include Barrow, Nome, Kotzebue, Dillingham, Cordova, Sitka, Petersburg, Wrangell, Ketchikan, Haines, Skagway, and Yakutat.

All Zone A, B and C locations are subject to zone classification change based on the economy of the area and the available manpower to service that area and is subject to a 30 day written notice.

B. Hawaii, Pacific Islands:

1. Service on products located in service Zone A will be charged at Xerox' then current FSMA or Time and Material rates.
2. An additional 25% surcharge will be added to the current FSMA or Time and Materials labor charge for service repairs performed on products located in Zone B.
3. Supplemental Zone C charges:
 - a) Customer Service Engineer round trip transportation expenses to machine location.
 - b) Customer Service Engineer food and lodging expenses.

4. ZONE DEFINITION

- ZONE A Islands of Hawaii, Oahu, Maui, Kauai, Guam S&L, Saipan S&L.
- ZONE B Guam Commercial, Saipan Commercial.
- ZONE C Islands of Molokai, Lanai, Tinian, Rota.

C. Continental Remote Locations:

Charges for Customer Service Engineer round trip transportation expenses and food / lodging expenses may be applicable.

Question # 6 Equipment Technical Service and Support -Describe how your Company will meet or exceed UC’s service guarantee commitments and credits for MFDs attached.

1. Service Guarantee Commitments

- a. Describe how the Company will meet UC’s service guarantee commitment requirements for digital MFDs below:

Description	Commitment
1. Service/Guarantee a) Total uptime (MFDs) b) MFD warranty (parts & labor)	a) 96% (not more than 8 hours of downtime per month based on the total number of working hours per month) b) 90 days - Total customer satisfaction guarantee
2. Response/Repair Time –MFDs a) Response time b) Response times to areas beyond 20 miles from major UC Locations	a) 4 business hours with 1 business hour acknowledging call back from technician or dispatch – starting from time of call placement b) Maximum 8 hours or upon mutually agreed time with field office or location administrators.
3. Delivery/Installation a) Delivery (new equipment) b) Delivery (replacement parts) c) Delivery (supplies) Installation	a) 10 business days from vendor receipt of order; delivery between 8am and 12noon (Pacific), with one hour pre-delivery call, unless otherwise arranged b) Within 8 business hours from vendor receipt of order c) Within 2 business days from vendor receipt of order d) Installation upon delivery, unless otherwise arranged
4. Setup	Within 4 business hours of delivery, unless otherwise arranged.
5. Training Initial Customer training and IT support	Unlimited user training on features and functionality at no charge. Initial IT - support no charge.
6. Customer Service a) 800 Number b) Return customer calls	a) At no cost b) Within 1 business hour

Service Guarantee Commitments, Delivery/Installation. Delivery. Please note the following will apply to any Purchase and Lease transaction: Unless otherwise agreed upon by the parties, Xerox equipment deliveries can normally be expected within ten business days following the receipt of the University’s equipment approved and accepted purchase order, except during times of product constraint. Xerox will inform the University if a constraint condition exists and will provide a revised delivery date. If the revised target delivery date is unacceptable, the University can cancel the order without penalty to either party. Accepted by Xerox?

Installation. Unless the Purchase and Maintenance and Lease Agreement is preceded by a Trial order, the equipment will be deemed accepted on the equipment’s installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University’s use. The Installation Date for equipment and software designated as “Customer Installable” will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox’s option a unit with similar capabilities and comparable usage.

Service Guarantee Commitments. Total Uptime Xerox's Uptime objective is to maintain an average 96% equipment uptime performance based on a three-month rolling average for the University's entire Xerox-branded equipment population that is operated with the equipment's operating guideline for the specified product. Uptime is calculated as follows:

- **Uptime target.** Provided Customer has at least twenty-five (25) units of Equipment installed under this Agreement, Xerox agrees to maintain an Uptime Target for the total Equipment population installed under this Agreement, which shall be measured as provided below over a three (3) calendar month rolling period, of at least ninety-six percent (96%) in the aggregate for the Equipment subject to this Agreement that is operated within the specified Maximum Monthly Volume Range, (to be included upon University's request in an Appendix to this Contract) and installed within twenty-five (25) miles of a Xerox service location. This Uptime Target commences on the first day of the calendar month that begins at least one hundred twenty (120) days after the Agreement commences.
- **Contracted period of coverage.** Xerox will provide Maintenance Services, as the same is set forth in this Agreement, during Customer's normal business hours Contracted Period of Coverage ("CPOC"), which shall be defined as 9:00 a.m. to 5:00 p.m., Local Time, Mondays through Fridays (excluding Xerox-recognized holidays), for the purposes of this Agreement.
- **Uptime hours definition.** "Uptime Hours" equals the number of hours per calendar month that the Equipment is available for use. For this Agreement, Uptime Hours equals 567 hours per three (3) calendar months and has been calculated by multiplying the number of hours per day in the CPOC times the average number of days per three (3) calendar month period such coverage is provided, which, for the purposes of this Agreement, is sixty-three (63) days per three (3) calendar month period..
- **Downtime hours definition.** "Downtime Hours" shall mean the number of hours in any three (3) calendar month period during which Equipment maintained hereunder is inoperative (i.e., cannot make any copies or prints, as applicable) during the CPOC, including machine-repair time and response time when the Equipment is inoperative. Downtime Hours do not include time when the Equipment's inoperability is due to user misuse or abuse of the Equipment, Customer's negligence or intentional acts, fire, environmental failure at the installation site or use of the Equipment in a manner other than was intended; preventative maintenance, Equipment relocation or inspections are being performed; and, time taken in producing usable copies or prints.
- **Calculation.** The Uptime Percentage Rate for a given calendar month is calculated as follows:

$$\text{Uptime Percentage Rate} = \frac{\text{CPOC (567)} - \text{Downtime Hours (x)}}{\text{CPOC Hours (567)}}$$

MFD warranty (parts and labor):

Purchase and Maintenance. Please note Xerox's proposal includes a 90 days no charge warranty (service/parts/supplies).

Lease. Please note that all of the Xerox-branded equipment is backed by Xerox's Total Satisfaction Guarantee Program, which allows the University, at its request, to replace any problem equipment with an identical model or, at the option of Xerox with a machine with comparable features and capabilities, and comparable usage. This guarantee will be effective for three years following the equipment's installation for purchased equipment that has been continuously maintained by Xerox or its authorized representatives under a Xerox express warranty or Xerox maintenance plan, and during the entire 60-month equipment Purchase and Maintenance and Lease term, except for equipment damaged or destroyed due to an Act of God. If the situation arises, where the equipment does not perform to its published specification and the University elects to exercise the Total Satisfaction Guarantee, Xerox agrees to meet with the University's representative and arrange a mutually agreeable time for the equipment's exchange.

Describe how your Company will meet or exceed UC's service guarantee commitment requirements for Laser Printers attached.

1.Service /Guarantee

- a) Total uptime - Laser Printers
- b) Printer warranty (parts & labor)
- c) 96% (not more than 8 hour of downtime per month based on total number of working hours per month)
- d) Standard 1 year or more

2.Response/Repair Time – Laser Printers

Response time Within 2 business days

3.Delivery/Installation

- a) Delivery (new equipment)
- b) Delivery (replacement parts)
- c) Delivery (supplies)
- d) Installation (optional)
- e) 10 business days
- f) Within 2 business days
- g) Within 2 business days
- h) If requested, within 2 business days of delivery, unless otherwise arranged.

4. Customer Service

- a) 800 Number
1-800-821-2797
- b) Return customer call
Within 1 business hour

a. Describe how the Company will meet UC’s service guarantee commitment requirements for Laser Printers below:

Description	Commitment
1. Service/Guarantee a) Total uptime - Laser Printers b) Printer warranty (parts & labor)	a) 96% (not more than 8 hour of downtime per month based on total number of working hours per month) b) Standard 1 year or more
2. Response/Repair Time – Laser Printers Response time	Within 2 business days
4. Delivery/IServicenstallation a) Delivery (new equipment) b) Delivery (replacement parts) c) Delivery (supplies) d) Installation (optional)	a) 10 business days b) Within 2 business days c) Within 2 business days d) If requested, within 2 business days of delivery, unless otherwise arranged.
5. Customer Service a) 800 Number b) Return customer calls	a) At no cost b) Within 1 business hour

Laser Printers.

Purchase and Maintenance. Please note Xerox’s proposal includes one year no charge Warranty for Printers under the “Outright Sale with Maintenance Offer” only.

Lease: For FMV/FPO leases the Maintenance is included and begins upon install.

Response/Repair Time. Xerox’s response time objective is to return all service calls within one business hour, and to arrive on-site on average within 3.5 to 4 business hours for multifunction color devices, if the problem cannot be resolved over the phone. **Response Time for other devices will be provided upon request.** Response time is calculated based on the quarterly response time average for the University’s entire Xerox-branded equipment population. Calls can be placed toll free 24-business hours per day, 7 days per week, and 365 days a year. During standard business hours (8 A.M. to 5 P.M., Monday thru Friday), all service calls will be directed to our Service Welcome Center where our service personnel will attempt to resolve the issue over the phone through on-line diagnostics. If the problem cannot be resolved over the phone the representative will provide the caller with the technicians estimated time of arrival. The Service Technician will contact the caller prior to arriving on-site to discuss the problem and determine if they have the appropriate parts, or if there will be a change to the arrival time. Evening, weekend, and holiday phone service is also available. On-site evening, weekend, and holiday service support can also be prearranged or may be available based on evening resource availability. The 24x7-call center and business hour technical support is included in our contract offering. After hour, weekend, and holiday on-site technical support is available at Xerox’s then current overtime rate. Please refer to the XPS Description of Services for response time objectives relating to the XPS / Managed Print Services offering.

Delivery/Installation.

Delivery. Please note the following will apply to any Purchase and Lease transaction: Unless otherwise agreed upon by the parties, Xerox equipment deliveries can normally be expected within ten business days following the receipt of the University's equipment approved purchase order, except during times of product constraint. Xerox will inform the University if a constraint condition exists and will provide a revised delivery date. If the revised target delivery date is unacceptable, the University can cancel the order without penalty to either party.

Installation. Unless the Purchase and Maintenance and Lease Agreement is preceded by a Trial order, the equipment will be deemed accepted on the equipment's installation date, which is the date Xerox determines the equipment to be operating satisfactorily, as demonstrated by the successful completion of diagnostic routines, and is available for the University's use. The Installation Date for equipment and software designated as "Customer Installable" will be the equipment delivery date. Any equipment that does not perform to its published specification will be repaired or replaced by Xerox at its expense, provided the equipment is covered by a Xerox warranty or maintenance plan. Any equipment that needs to be replaced will be replaced with an identical model, or at Xerox's option a unit with similar capabilities and comparable usage.

Option #1 and #2 will be covered by our Full Service Maintenance Agreement. Detailed pricing has been provided in the UC worksheets. Please note that all of our prices, options, accessories, etc. could not be input into the worksheet due to limited or locked cells. The full Xerox price list has been included in the response for your review and analysis. Please refer to d Xerox Price Addendums.

Option #3 – T&M

Printers

Call charge \$314.00

Labor Rates per additional 15 minutes \$72.00

After hours Monday - Saturday \$123.00

Sunday \$152.00

MFD

Call charge \$ 437.00

Labor Rates per additional 15 minutes \$79.00

After hours Monday - Saturday \$136.00

Sunday \$168.00

Please refer to **Attachment - T&M Pricing.pdf**.

Full Service Maintenance Agreement

A Xerox Full Service Maintenance Agreement (FSMA) maximizes your productivity and ensures your investment in technology pays off. Standard service coverage hours are from 8 A.M. until 5 P.M., Monday through Friday, excluding designated holidays. Xerox FSMA includes all parts, labor, software updates, maintenance and travel for your product's operating hardware and software. A 24x7 support staff to assist with your hardware or software problem resolution, software version updates, hardware retrofits and all diagnostic licenses are also included. Additionally, our Professional Services provide access to fee-based onsite System Analyst support. If Xerox cannot repair your product to full working order, Xerox will ensure you receive a comparable replacement product with an identical model or one with comparable features and capabilities. The FSMA is very flexible and can be customized in a number of ways (additional fees may apply):

Extended Shift FSMA: If you require after hours coverage and maximum uptime, this plan is best for you. It provides you all the benefits listed above, plus expanded coverage with eight different shift coverage options based on the number of days per week and shifts per day, up to 24/7.

XTend Agreement: This option is an excellent choice if you require holiday coverage and/or unique, nonstandard coverage. It enables you to customize your FSMA to meet your mission-critical needs, for example, if you need weekend coverage for a month or second-shift coverage for a week.

Xerox understands and will comply with all requirements.

For situations that need immediate personalized telephone support, you can call the North American Customer Support Center (NACSC). Our team of over 600 professional and friendly Customer Support Representatives (CSRs) provides one-to-one expert advice over the phone during contracted hours of support. You can call the NACSC toll-free at 1-800-821-2797 for Office and Production Equipment and 1-800-836-6100 for Phaser® and Network Printers. Our goal is to answer within 90 seconds. A CSR answering your call reviews the problem with you over the phone and will provide recommendations for immediate remote resolution of the problem. Our skilled staff at the NACSC is able to solve up to 25 percent of all calls remotely. If onsite service or escalation to second-level support is needed, these are completed within your contracted hours of support.

Remote Support Engineers (RSEs). Xerox RSEs provide second level support to both our customers and our CSEs. They are available via the phone and onsite (for some products) as necessary within contracted hours of support. They have access to Design Engineering for escalation and the latest fixes to help you with complex problems or to help our CSEs restore your equipment as quickly as possible. The goal for telephone response from Level 2 is within a minute for Production Equipment and five minutes for Office Products.

One of the truly unique aspects of Xerox Support is the use of Design Engineers to assist in supporting our customers. Design Engineers are readily available to assist in the resolution of escalated customer issues and to continue to improve the performance of every machine in the field. The close relationship between our CSEs and Design Engineers allows issues to be discovered at your site and be escalated to Design Engineers for an immediate product retrofit. Sometimes this discussion will lead to a next-generation improvement. For certain types of technical problems, Design Engineering will work with the local service team to determine whether an onsite problem-solving visit by an engineer is required.

It is Xerox's goal to ensure you are totally satisfied. In support of that goal, our simple closed-loop service call process has been designed to resolve any problems that may arise, or any issues you may have with regards to your Xerox product, to your satisfaction as quickly and effectively as possible. The steps in the service call process are as follows:

- The process begins by placing a call to Xerox's Customer Support Center (CSC) at 1-800-821-2797 for Office and Production Equipment and 1-800-836-6100 for Phaser and Network Printers.
- The Customer Support Representative (CSR) who answers your call will ask you for the equipment serial number as well as a contact name and phone number. The CSR will then assess your problem and, if possible, make recommendations to immediately resolve your problem remotely.
- Office Equipment: If remote resolution is not possible, the CSR will give the Office customer an Estimated Time of Arrival (ETA), and the CSR will send an automatic page to a Customer Service Engineer (CSE) assigned to your area to alert him/her that a service call is required at your facility. **CSEs that support Office products will have a queue for remote solve calls. These calls will be forwarded to a dedicated CSE, who will call the customer and attempt remote solve within one hour.
- Production Equipment: Within one hour of your call to the CSC, the dispatched CSE will contact you or the contact person you have identified. At that time they will verify your contact name and phone number, verify the equipment issue, gather your requirements and provide an estimated arrival time. If possible, given the nature of your problem, the CSE may recommend clearance procedures or other steps for you to take in an effort to get you up and running.
- Office and Production: Upon arrival at your site, the CSE will review the equipment issue with you and give you an estimate of the time required to repair your equipment.

- The CSE will then repair your equipment. While there, the CSE will check the overall operation of your equipment, perform any preventative maintenance required, and run a thorough system check.
- After completing these activities, the CSE will review the repairs made with you to ensure your satisfaction. If follow up is required, the CSE will work with you to establish a convenient follow-up date and time.

Supplier name here:

--

Instructions:

(A). Enter your company name in the yellow cell above.

(B). If you have done business with UC in the last 2 Fiscal Years FY 2018 (July 1, 2017 –June 30, 2018) and FY 2019 (July 1, 2018 –June 30, 2019), populate each tab with UC Historical

(C). Tabs

*FY'18 MFDs

*FY'18 Laser Printers

*FY'19 MFDs

*FY'19 Laser Printers

Note: Please Do Not change any of the existing row and column headers.

UC FY 2019 Historical Purchases (MFDs)

July 1, 2018 - June 30, 2019

Multifunction Devices	Monochrome				Color			
	Purchases	Leases	Services	Other (accessories, parts, supplies, etc.)	Purchases	Leases	Services	Other (accessories, parts, supplies, etc.)
UCB		\$ 162,274.11	\$ 19,253.98					
UCD		\$ 250,776.95	\$ 2,398.78					
UCI		\$ 1,030,938.91	\$ 68,050.86					
UCLA		\$ 970,512.71	\$ 52,214.57					
UCM		\$ 29,379.11						
UCR		\$ 83,925.13	\$ 6,511.01					
UCSB		\$ 55,453.68	\$ 144.02					
UCSC		\$ 3,089.40						
UCSD		\$ 552,646.87	\$ 18,429.14					
UCSF		\$ 643,383.08	\$ 746,384.40					
UCOP			\$ 74,250.86					
LBNL								
UCIMC		\$ 2,186.49						
UCDMC		\$ 5,072.14	\$ 238,163.56					
UCLAMC		\$ 11,850.81						
UCSDMC								
UCSFMC		\$ 18,224.40						
UC Hastings			\$ 1,714.94					

UC FY 2018 Historical Purchases (Laser Printers)

July 1, 2017 - June 30, 2018

Laser Printers	Monochrome			Color			
	Purchases	Services	Other (accessories, parts, supplies, etc.)	Purchases	Leases	Services	Other (accessories, parts, supplies, etc.)
UCB							
UCD							
UCI							
UCLA							
UCM							
UCR							
UCSB							
UCSC							
UCSD							
UCSF							
UCOP							
LBNL							
UCIMC							
UCDMC							
UCLAMC							
UCSDMC							
UCSFMC							
UC Hastings							

UC FY 2019 Historical Purchases (Laser Printers)

July 1, 2018 - June 30, 2019

Laser Printers	Monochrome			Color			
	Purchases	Services	Other (accessories, parts, supplies, etc.)	Purchases	Leases	Services	Other (accessories, parts, supplies, etc.)
UCB							
UCD							
UCI							
UCLA							
UCM							
UCR							
UCSB							
UCSC							
UCSD							
UCSF		\$ 57,610.00					
UCOP							
LBNL							
UCIMC							
UCDMC							
UCLAMC							
UCSDMC							
UCSFMC							
UC Hastings							

3.1 Company

A. Brief history and description of Supplier.

History: The roots of Xerox Corporation go back over 100 years to our humble beginnings as the Haloid Company, established in 1906. In that time, we pioneered and brought to market many of the technologies and solutions used by office workers every day.

From the first xerographic image made in 1938 to breakthroughs in home and business computing during the 1970's and our influence and leadership in shaping the current Managed Print Services (MPS) offering; to delivering our "game changing"

ConnectKey® Technology, which enables modern workers to leverage Xerox® Multifunction Devices (MFDs) to simplify the way work gets done in the office and on the go.

Xerox Today: With annual revenues of \$9.8 billion we are a leading global provider of digital print technology and related solutions; we operate in a core market estimated at approximately \$67 billion. Our primary offerings span three main areas: Intelligent Workplace Services (formerly Managed Document Services (MDS)), Workplace Solutions and Production Solutions (formerly Graphic Communications). Our Intelligent Workplace Services offerings help customers, ranging from small businesses to global enterprises, optimize their printing and related document workflow and business processes. Xerox led the establishment of this expanding market and continues as the industry leader. Our Workplace Solutions and Production Solutions offerings support the work processes of our customers by providing them with solutions built upon our broad portfolio of industry-leading printing and workflow offerings. We also have digital solutions and software assets to compete in an approximately \$31 billion adjacent Software and Services market. Our main offerings for this market are focused on industry-specific Digital Solutions, Personalization & Communication Software and Content Management Software. Headquartered in Norwalk, Connecticut, with 32,400 employees, Xerox serves customers in approximately 160 countries providing advanced document technology, services, software and genuine Xerox supplies for a range of customers including small and mid-size businesses ("SMB"), large enterprises, governments and graphic communications providers, and for our partners who serve them. To learn more, visit us on Xerox.com, Xerox Innovation History and Xerox Today.

Xerox Research and Innovation

We believe that a critical role of our research is to identify new competency areas with attractive addressable markets for the future. Our expertise in technology and printing uniquely positions us to discover those areas and leverage our innovation to move into adjacencies beyond our current core technology. Accordingly, we have prioritized investments in four key areas: Digital Packaging and Print, AI Workflow Assistants for Knowledge Workers, 3D Printing / Digital Manufacturing, and Sensors and Services for the Internet of Things. We also see opportunity in our core coming from our ability to deliver physical devices that connect with the digital world as well as purely digital offerings that improve our customers' outcomes. As a result, we direct our research and development (R&D) investments to areas such as workflow automation, color printing and customized communication, as well as to improving the quality and reducing the environmental impact of digital printing. We invest in bringing new capabilities to the market such as our ConnectKey™ software to enable our devices to integrate into digital workflows, as well as in technologies to improve the security of our devices and offerings. We will continue to invest in innovations to improve the reliability, IQ and cost of our printing devices, as well as in new services and software that improve our customers' ability to manage their document-oriented workflows.

Xerox Values

Keeping connected to our core values helps us to execute our priorities and strategies and fulfil our mission of delivering excellence to our customers, our shareholders and each other. They are a part of our heritage and are a part of our future.

Since our inception, we have operated under the guidance of six core values:

- We succeed through satisfied customers.
- We deliver quality and excellence in all we do.
- We require premium return on assets.
- We use technology to develop market leadership.
- We value and empower employees.
- We behave responsibly as a corporate citizen

B. Total number and location of sales persons employed by Supplier.

Xerox has a nationwide sales organization that is aligned to a geographic focus and is primarily aligned on the basis of go-to-market sales channels, which are structured to serve a range of customer for our products and services. We employ 1450 sales resources across the United States, covering virtually every metropolitan area. There are three primary sales channels that cover public sector agencies nationally.

- Xerox Direct Enterprise: Under the leadership of regional Vice Presidents, Xerox has Sales Professionals across the United States that focus on providing Xerox's innovative product and services portfolio to large State Government agencies.
- Xerox Business Solutions (XBS): A wholly owned unit of Xerox Corporation, XBS is comprised of a nationwide network of companies (all wholly owned by Xerox) that provide Xerox Sales and Services throughout the US.
- Authorized Xerox Sales Agencies: Independent Sales Agents that exclusively represent Xerox with access to Xerox products and services for small and medium businesses.

Please refer to **Attachment A** for a complete list of all U.S. Sales offices.

C. Number and location of support centers (if applicable) and location of corporate office.

Support Centers

Customers enjoy unlimited access to the Xerox Welcome Center for technical issues, supplies or billing Inquiries. The Welcome Center provides online support and phone access to our multi-lingual support team. You can contact the Xerox Welcome Center at 1-800-821-2797 (US only). For more assistance, please visit www.support.xerox.com.

Our Customer Business Center is another point of contact for customers to call for technical service/repair, make a payment, self-service options (receive copy of an invoice, account balance, Address change form, contract date, status of supply order), billing, obtaining quotes, etc. Our Customer Care and Support team can be reached at 1-888-771-5225.

Corporate Office

Our registered corporate office address for company headquarters is: Xerox Corporation, 201 Merritt 7, Norwalk, Connecticut 06851.

D. Annual sales for the three previous fiscal years.

- 2017 Annual Gross Sales: \$ 9,991 billion
- 2018 Annual Gross Sales: \$ 9,662 billion
- 2019 Annual Gross Sales: \$ 9,066 billion

E. Submit FEIN and Dunn & Bradstreet report.

FEIN

Xerox FEIN: 16-0468020.

Dunn & Bradstreet Report

Please refer to **Attachment B** for Xerox' s Dun and Bradstreet report. D&B Supplier Qualifier Report-Xerox.

F. Describe any green or environmental initiatives or policies.

The Xerox Business Code of Conduct for Corporate Social Responsibility is Xerox's overarching policy from which policies covering social, environmental and economic dimensions are referenced as shown below. For expansive detail on Xerox CSR, please see <https://www.xerox.com/en-us/about/corporate-social-responsibility>

Environmental Policies:

- EHS 100 Environment, Health, Safety & Sustainability
- EHS 101: Environment, Health and Safety Policy for Xerox Workplaces,
- EHS 102: Environment, Health & Safety Policy for Products and Materials

Social Policies:

- POL 002: Business Ethics
- OGC 020: Relationships with Government Customers & Officials and Political Contributions
- InfoPriv 001: Personal Information Privacy
- InfoPriv 003: Requirements for Commercial E-mail Messaging
- SEC 003: Physical Security– General Policy
- InfoSec 001: Information Security
- HR 101-1: Outside Business Interests and Conflict of Interest
- HR 107.1: Employee Communications – Open Door/Internal Escalation Process
- HR 201.0: Employment, Placement, & Separations: Non-Discrimination
- HR 201.3: Equal Opportunity, Non- Discrimination, & Harassment
- HR 503: Alcohol and Drug Misuse
- HR 105: Recognition, Recreation and Social Activities
- SEC 009: Violence-Free Environment
- InfoPriv 001: Personal Information Privacy
- POL 007: Human Rights
- HR102: Civic and Political Activities
- HR 103: Solicitation of Employees
- OGC 022: Global Corporate Philanthropy Policy
- OGC 023: Global Volunteer Policy

Economic Policies:

- ACC 208: Code of Conduct Finance Personnel
- ACC 1207: Revenue Recognition
- PUR 001: Purchasing Policy
- SRY 001: Purchasing and Selling Xerox Securities By Employees, Officers and Directors
- OGC 019: Compliance with Antibribery Laws

Please describe Environmental Initiatives:

Our various environmental initiatives extend across our supply chain, product lifecycle and operations and are described at <https://www.xerox.com/en-us/about/ehs>.

These include:

- Commitment to the Responsible Business Alliance (RBA) Code of Conduct for our Operations and Suppliers. Our suppliers must meet Xerox's strict standards to control the chemical content of our products. Xerox is a member of the **Responsible Business Alliance (RBA)** which has developed a standards-based approach for monitoring suppliers' compliance across several areas of social responsibility, including labor, health, safety and environmental activity.
- Design for Sustainability- A cornerstone of our design is meeting the certification of premier eco labels including EPA Energy Star, Electronic Product Environmental Assessment Tool (EPEAT) and the German Blue Angel. Our Cleantech plank will use Xerox technologies to deliver environmental, social and economic benefits to current industrial processes.
- Corporate-wide science-based energy and GHG goals to reduce energy consumption and GHG emissions by 85 percent by 2030 (from a 2002 baseline).
- Through our partnership with **PrintReleaf**. Xerox customers have the opportunity to contribute to the reforestation of global forests and reduce their overall sustainability footprint. Based on a theme of "You print one, we'll plant one," paper usage reporting is used to equate the number of trees that are reforested into geographic areas of need.
- Software products such as DocuShare® and FreeFlow® Digital Workflow Collection help Xerox customers reduce paper consumption by facilitating electronic data management, scan-to-e-mail, print-on-demand and distribute-then-print workflows.
[Office software solutions ›](#)
[Production software solutions ›](#)
- The Xerox **Green World Alliance** collection and reuse / recycling program in partnership with our customers, results in millions of cartridges and toner containers returned for reuse or recycling each year.
- Xerox joined the Sustainable Electronic Recycling International coalition as a founding member of the "R2 Leader Program". **SERI** is a non-profit organization devoted to advancing sustainable electronics reuse and recycling globally. R2 Leaders commit to supporting responsible and sustainable electronics repair and recycling as described in the R2 Standard. Additionally, R2 Leaders, including Xerox are taking leadership roles in projects for responsible reuse and recycling around the globe.

G. Describe any diversity programs or partners supplier does business with and how Participating Agencies may use diverse partners through the Master Agreement. Indicate how, if at all, pricing changes when using the diversity program.

As a global leader in business process and document management, Xerox recognizes that having a diverse supplier pool is a major competitive advantage and a powerful business tool. Xerox's Supplier Diversity Program's mission is to proactively identify, build relationships with, and purchase goods and services from certified small businesses as well as enterprises owned by minorities, women, veterans, gays and lesbians, and disabled persons that can help Xerox achieve its corporate objectives as suppliers to Xerox. Also, through Xerox's dedicated Divers Alliance Program, we are committed to understanding and supporting our customer's supplier diversity goals and objectives. Specifically, Xerox in connection with the University of California Master Agreement will support OMNIA Members by offering solutions which include certified HUBs or other certified diverse subcontractors as part of our offer where applicable and practical. While Xerox is not a certified diverse company, we believe selecting Xerox would give OMNIA Members the best of both worlds by working with the leading global document management company which is committed to having practical and useful diverse certified subcontractors directly supporting our contract with you.

H. Describe any historically underutilized business certifications supplier holds and the certifying agency. This may include business enterprise such as minority and women owned, small or disadvantaged, disable veterans, etc.

Xerox is not a certified diverse company; however, we do work with certified diverse companies to provide direct and indirect spend as part of our offer to our customers.

I. Describe how supplier differentiates itself from its competitors.

Today's Xerox is a leader in print technology and intelligent work solutions using the advantages of our people, our approach, and industry leading technology to solidify our stronghold in a number of competitive markets.

Our Approach

- We have deep industry knowledge and take the time to understand our clients' business and how they work, to build and create solutions – to help them achieve their goals.
- We work with clients to innovate, incubate and explore new solutions to critical business challenges.
- Using user centric design, we study how people work in order to make it better.
- We know every workflow is different, so we strive to create solutions that match each need.

Our Market Position

- MPS Market share leader and thought leader according to leading Industry Analyst Firms.
- Xerox is the most decorated and experienced vendor in the Managed Print Services Landscape. All three major industry analysts, (Quocirca, IDC, InfoTrends) have placed Xerox as the top provider in the MPS landscape in their most recent market reports.
- We maintain our No. 1 position in worldwide equipment sales revenue and No. 1 marketshare in production color.
- Managing billions of printed pages per year with unparalleled global delivery.
- Tight integration with technologies used by today's workforce enabling access to cloud-hosted services, exceptional customized experiences, and maximum productivity.

Our People

- We never give up – whether it is providing support to customers, developing a better way to help customers work better, or pushing the limits of technology and software innovation.
- We believe collaboration and teamwork are the only way to achieve success.
- We attract, hire and retain the top talent with the best skills.
- Named one of the World's Most Ethical companies by Ethisphere Magazine, for 12 consecutive years.
- Listed as one of the World's Most Admired Companies by Fortune Magazine.

Our Technology and Innovation

- World-renowned innovation and expertise – including printing, advanced color science, digital and video imaging, workflow automation, connectivity, and analytics.
- We are innovators and inventors and our people have over 10,307 active patents. Xerox is one of the top 20 patent producing companies in the world.
- Over \$1 billion is invested in R&D and engineering each year.
- Xerox has been the force behind many major technology breakthroughs – such as the ConnectKey interface and the adaptive color technology – which have transformed how work gets done.

Security Protocols Providing the Upmost Protection for our Customers

- Multifunction devices are sophisticated, multiple sub-system network platforms, and Xerox offers the broadest range of security functionality on the market, including encryption, authentication, authorization per user and auditing.
- ISO 15408 Common Criteria for Information Technology Security Evaluation is the only internationally recognized standard for security certification. Xerox was the first manufacturer to seek and obtain certifications for “complete” MFP devices. Because each element of the multifunction platform is a potential point of entry, meaningful security certification must comprehend all elements, including the operating systems, network interface, disk drive(s), Web server, PDL interpreter(s), MFP user interface, local hardware ports and fax system.
- Users of Xerox® ConnectKey® Technology-enabled ‘i-Series’ Smart MFPs also now have the option to encrypt PDF files with a password when using the Scan to Email service allowing only authorized users to see documents.
- From the introduction of the first digital products, Xerox has recognized the risk of retained data being inappropriately recovered from non-volatile storage and built features and countermeasures into our devices to help customers safeguard their data.
- Many Xerox® devices include features to protect the printer or MFP from unauthorized remote access, protect the confidentiality of data transmitted to the device via the network, control which devices can access the MFPs and control the ports, protocols and services that can be accessed on the device.

J. Describe any present or past litigation, bankruptcy or reorganization involving supplier.

Xerox is a large, global enterprise with thousands of contracts with vendors, customers, business partners and other parties. At any given time, there may be issues that could possibly result in lawsuits or other legal actions. Producing a detail list of such activity would be onerous in the context of responding to this RFQ. However, any material litigation or judgments against Xerox can be found at [www/Xerox.com](http://www.Xerox.com) at Investor Relations.

Xerox has not been part of any bankruptcy procedures.

K. Felony Conviction Notice: Indicate if the supplier

a. is a publicly held corporation and this reporting requirement is not applicable;

Xerox is a publicly held corporation.

b. is not owned or operated by anyone who has been convicted of a felony; or

Xerox is not owned or operated by anyone who has been convicted of a felony.

c. is owned or operated by and individual(s) who has been convicted of a felony and provide the names and convictions.

Xerox is not owned or operated by anyone who has been convicted of a felony.

L. Describe any debarment or suspension actions taken against supplier.

Xerox is a large, global enterprise with thousands of contracts with vendors, customers, business partners and other parties. These contracts are amended, renewed, and terminated on a regular basis for a variety of reasons and Xerox does not maintain records regarding the reasons for such routine contract administration matters. However, the termination of any material agreement is disclosed in the periodic reports filed by Xerox with the U.S. Securities and Exchange Commission ("SEC"). These reports are available at www.sec.gov/edgar.shtml.

Xerox has not been disbarred, suspended or otherwise disqualified from doing business with the federal government.

3.2 Distribution, Logistics

A. Describe the full line of products and services offered by supplier.

We provide the industry's broadest portfolio of document technology and software. Through our innovation and market leadership, we have developed a strong industry reputation and recognizable brand with trusted competencies in bridging the physical and digital printing and communications, both in the office and productions markets. Our core capabilities and offerings consist of technologies, solutions and services that simplify workflows, grow revenue and transform the customer experience, as described below.

Xerox Technology and Software – Workplace Solutions

Entry Desktop Monochrome and Color Printers

Entry Desktop Monochrome and Color Printers range from small devices to workgroup printers and MFPs that serve the needs of office workgroups. These products help build a platform to effectively manage document workflow.

Mid Range

Our Mid-Range products offer advanced features with the ability to handle higher print volumes as well as varying paper sizes. Entry and Mid-Range products share common technology, manufacturing and product platforms enabling ease of use and complete office integration.

Software Platform

What makes Xerox Printer/Multifunction Printer (MFP) unique is that they are built on the Xerox ConnectKey Technology platform. This platform enables a Process for Workflow improvement. It operates with an intuitive-like touchscreen user interface. The platform is an open embedded platform that allows the device to be programmed to address specific workflows. This new capability is driven by embedded or server-based software inside the firewall or in the cloud. As such, the smart Printer/MFP incorporates an ecosystem of hardware, software, and services to address public agency's document and information processing requirements.

Managed Print Services

MPS is at the core of what Xerox is today. It is a service that combines traditional document output technology with a services backbone that allows customers to focus on their core competencies while helping clients to cut cost, increase productivity and meet their environmental sustainability goals. As a leader in MPS, Xerox offers a full range of Managed Print Services to embrace all elements of an organization's print infrastructure—from the networked office to the in-house print center to the virtual worker. Founded on rigorous, data-driven Lean Six Sigma-based methodologies, the Xerox Managed Print Services portfolio extends from global enterprises to small and mid-sized businesses.

Xerox has several different approaches to Managed Print Services. All Xerox Managed Print Solutions incorporate an assessment of the current state of the environment and then recommendations for a proposed future state. The assessment typically gathers data on the customer's current fleet which may include current costs, application requirements and other pertinent information to the clients environment as agreed upon. The data gathered from the current state will be used to develop a proposed future state with proposed costs of an MPS solution and any potential cost savings.

The proposed future state typically includes the customer's output fleet of devices under an umbrella management contract which includes break/fix, help desk services, supplies, management reporting, proactive problem resolution, etc. Xerox also offers additional optional services as outlined within the response.

Xerox Managed Print Services solutions can be contracted for at a fixed price per unit or a per page cost depending upon the size and scope of the engagement. These services are configured based on individual customer requirements, therefore, we do not have list prices for these services. The attached price list provides a not to exceed price for the range of services associated with Managed Print. There are two discreet price lists for two discreet offerings, Xerox Print Services (XPS) and Enterprise Print Services (EPS).

XPS is an entry level Managed Print offering that can utilized to manage an in-place multi-vendor printer environment. It can also be used to managed mixed environments of Xerox MFPs/Xerox printers and non-Xerox printers. XPS would be used where the customer intends to acquire Xerox MFPs from the University of California contract using Region 4 ESC contract pricing and terms and then incorporate the Xerox MFPs into a multi-vendor Managed Print Solution.

EPS is a more advanced Managed Print offering that is designed to support larger enterprise fleets and offers greater flexibility with respect to pricing options and contract terms. EPS also provides additional services offerings related to Managed Print such as onsite DocuCare Associates, Xerox Print Awareness Tool , etc. EPS can be offered on a fixed price basis or a cost per page basis.

In most cases, actual customer prices will be lower than the prices offered on the following XPS and EPS not to exceed price list. The initial assessment is used to develop actual data on current printer models and costs, actual volumes, potential savings and final pricing.

Xerox MPS Solution Deliverables

Outsourcing MPS requires a very specific, complex and customized approach involving people, process and technology tailored to each company and its unique requirements. Consequently, the process does not lend itself to a one-size-fits-all solution. It requires an experienced business partner like Xerox to manage the components in a simplified manner.

The Xerox MPS solution will deliver the following:

- **Assessment:** An MPS print assessment is the first step to help customers gain control, drive down print costs and improve productivity. The Assess and Optimize stage of Xerox® Managed Print Services leverages our award-winning managed print services assessment processes and tools. Xerox® Asset DB and CompleteView™ Pro turn print data into actionable knowledge to control and drive down costs, while reducing your environmental impact. With a complete and secure analysis of print usage and costs, we help customers understand the total cost of ownership and a more efficient print environment. Xerox® CompleteView™ Pro can significantly reduce the time and effort it takes to gain valuable, comprehensive and accurate knowledge about your print environment.
- **Device Maintenance:** Including normal break-fix management services and the parts that are required to maintain devices in accordance with Original Equipment Manufacturer (OEM) specifications. Services include dispatching Xerox and/or third-party vendors, tracking all service calls through call resolution and reporting all associated maintenance services.
- **Asset Management:** Xerox has developed a centralized database of currently installed Xerox output devices to track the physical location and costs associated with each device. The services require an integrated approach focusing on the Client and Xerox working together to maintain the information. With the support of the Client IT, Xerox will implement technology to monitor the installed Xerox network-attached SNMP-Level 3 devices, and have integrated this monitoring technology with an SQL-based asset management database.
- **Consumables Management:** Xerox and the Client will agree on those processes for end users to order appropriate consumables. With these mutually agreed processes, Xerox will be able to consistently evaluate and provide the appropriate level of quantities of consumables at each of the Client's location to minimize end-user disruption.
- **Help Desk Support:** The client and Xerox will develop workflow processes that allow for help desk services and consumables for all in-scope devices as well as any services agreed upon by both parties. Utilizing the Xerox technology, we will proactively monitor in-scope devices. The Xerox Helpdesk agents will take the necessary action to ensure end-users have access to the full capability of the installed output devices. Those actions include dispatching appropriate break/fix resources to repair hardware, ordering and shipment of consumables and also contacting the Client's Service desk for application or network issues.

The services above will be documented in a formal Statement of Work (SOW) and will be managed to Service Level Agreements (SLA's) governing all key aspects of the program

- **Xerox Tool Suite**

The heart of the Xerox MPS solution is the Xerox Tool Suite — a set of Xerox proprietary software tools that provide comprehensive asset management, service support, reporting and problem management tracking services. The Xerox Tool Suite will integrate with Xerox people, process and technology to keep the Client's MFP's and printers running at peak performance, lowering costs as it improves productivity.

Getting timely and accurate reporting on fleet performance is a critical enabler to ensure that Xerox meets its agreed financial objectives and SLAs. With the Xerox Tool Suite, users can access real-time data to track how well we are responding when devices run out of supplies or machines jam or need service. The Xerox Tool Suite tracks how long the devices are down and when they are restored. When calls come in to the Help Desk, incident records are generated and tracked through resolution.

The Xerox Tool Suite continuously monitors the fleet and provides device status and device alerts. Xerox often proactively resolves service issues before the client even know there is a problem, allowing employees to focus on business, not on device-related issues.

Additional MPS options include:

Optimization of the Print Environment is an optional component under the Xerox MPS offer. Optimization of the print environment Includes floor analysis to map out current devices and volumes on the floors, identification of any physical departmental constraints, determination of specific application devices as reported by end users and client management, and identification of the specific move/add/change processes currently supported. Through our analysis, we provide the recommended future state optimized floor plans, which reposition devices to support end user requirements and reduce non-required devices from the floors.

On-site Support / DocuCare is an optional component under the Xerox MPS offer.

Xerox on-site support, or DocuCare, serves as the primary contact for equipment support and service. They coordinate Move/Add/Change/Delete process and may compliment the primary web based training for end users.

In addition, the resource serves as the first point of contact for Help Desk issues, provides basic cleaning and replacement of operator accessible parts and consumables, and first level break fix activities. Basic equipment problem diagnosis, IP address support, and the triage focal with Xerox help desk and technical support.

Xerox Services Portal (XSP) is an optional MPS component. The Xerox Services Portal (XSP) provides a customer interface to the Xerox Services information and reporting. It provides a secure website portal enabling customers to request supplies, service or MACD for their devices. XSP also allows end-users to access device training and feature information, find printers, submit meter reads, and deliver feedback on their equipment or MPS experience.

Xerox Consulting Services are optional Xerox MPS components.

Xerox Consulting Services provide two levels of support:

- Sr. Consultant Level - This is to provide senior, strategic and/or management level services associated with delivery of Managed Print Solutions. These include project management, transition management, change management, implementation management and services management.
- Consultant Level - This is to provide first line services including data collection, transition services, asset coordination, and implementation execution.

Xerox Print Security Audit Service (XPSAS) is an optional MPS component. is a comprehensive device security solution that incorporates risk mitigation services into an automated software tool. XPSAS brings automated remote configuration to device security. Xerox Print Security Audit Service automates setting device configurations remotely, monitors for compliance and remediates any violators in 3 key areas – firmware upgrades, password management and device settings configuration and management. Automation enables installation and delivery teams to reduce errors, save time and provide higher security levels to clients. Teams can demonstrate alignment to compliance standards using interactive dashboards – a unique advantage that comes only with Xerox.

User Analytics Service is an optional Xerox MPS component.

As Managed Print Services (MPS) environments mature, calculating the return on your investment is more complicated, and analytics become critical. Through analytics, organizations can capture and analyze data from various Print Management Solutions to make key decisions in the MPS environment. Furthermore, as employees continue to drive the usage of smartphones and tablets, user analytics can inform an organization on how to respond to an increasingly digital workforce in your organization. Understanding how users drive document output is the starting point for optimizing and automating the processes behind volumes. Customers uncover specific opportunities to capture savings, improve fleet efficiency and sustainability, tighten information security, increase productivity and drive digital transformation.

A few of the key benefits are the ability to identify areas of MPS competency and opportunities for improvement, obtain a plan and roadmap with Xerox to achieve your goals and gain insight into the value of MPS services available.

B. Describe how supplier proposes to distribute the products/service nationwide. Include any states where products and services will not be offered under the Master Agreement, including U.S. Territories and Outlying Areas.

Xerox sells our products and services directly to public agencies nationally through our national sales force, our authorized independent agents and our wholly-owned subsidiary, Xerox Business Solutions (XBS), formerly Global Imaging Systems (GIS), an office technology dealer comprised of regional core companies in the U.S. Our products and services can be offered in all 50 States, the District of Columbia as well as Guam, Puerto Rico and the Northern Marina Islands.

C. Describe how Participating Agencies are ensure they will receive the Master Agreement pricing; include all distribution channels such as direct ordering; retail or in-store locations, through distributors, etc. Describe how Participating Agencies verify and audit pricing to ensure its compliance with the Master Agreement.

Xerox Corporation utilizes multiple sales channels to market our products and services. This includes Xerox Direct Enterprise sales force, Authorized Xerox Agents and all XBS, a wholly owned subsidiary of Xerox Corporation. All orders and PO's under the UC Procurement Services contract will be processed through the Xerox centralized contracting system no matter which sales channel is making the sale. This ensures both consistency across all sales processes throughout the US and that all orders placed are compliant with the terms and conditions and negotiated pricing agreed to by Xerox and the University of California. As per the University of California's requirements, Xerox will provide quarterly reports including billed revenue.

D. Identify all other companies that will be involved in processing, handling or shipping the products/service to the end user.

As an integral part of the Xerox Supply Chain Network, Ryder Solutions is our largest 3rd party logistics partner involved in delivering equipment, parts and supplies. The Ryder relationship with Xerox has evolved over the past few decades in response to a changing transportation environment and Xerox's process requirements. Today, Ryder operates 5 distinct supply chain functions in the process: Several Carrier Logistics Centers, District Parts Center, Truckload (over the road) Transportation, Drayage of ocean containers and management of our LTL network.

The Carrier Logistics Center (CLC) network, made up of 51 locations and 17 different third party carriers (10 continental US and 7 offshore) involves the delivery, installation and removal of more than 100,000 imaging machines per year, where CLC drivers are trained in product installation, testing and removal. Flawless, seamless execution are essential to deliver outstanding service to Xerox customers.

CLC "Final mile" companies potentially involved in this business in addition to Ryder would include Fidelitone, All Points, Apex, Monarch/NET, Nationwide Electronics, Redman Van & Storage, Safeway/Unigroup, Sullivan Moving, WDS as our "onshore" or continental locations, as well as Reliable Transfer and Carlile Transportation in Alaska. We have delivery partners in Hawaii, Guam, Saipan, Puerto and the US Virgin Islands.

E. Provide the number, size and location of Supplier's distribution facilities, warehouses and retail network as applicable.

Within the America's Equipment Supply Chain, our primary distribution warehouse is in Indianapolis, IN. We have an additional six locations within the US where we hold inventory in our XBS facilities under centralized stock.

Below is a listing of the locations and size of these distribution sites.

Address	Size
3747 Plainfield Road - Suite 198, Indianapolis, IN 46321	770k sf
5700 WARLAND DRIVE, CYPRESS, CA, 90603	29k sf
10 Capitol St, Nashua, NH 03063	20.5k sf
17280 Green MTN Road, Ste. 130, San Antonio, TX 78247	48k sf
3 Territorial Court Bolingbrook, IL 60440	65k sf
10690 John Knight Close Montgomery AL 36117	20k sf

3.3 Marketing and Sales

A. Provide a detailed ninety-day plan beginning from award date of the Master Agreement describing the strategy to immediately implement the Master Agreement as supplier's primary go to market strategy for Public Agencies to supplier's teams nationwide, to include but not limited to:

- i. Executive leadership endorsement and sponsorship of the award as the public sector go-to market strategy within first 10 days
- ii. Training and education of Supplier's national sales force with participation from the Supplier's executive leadership, along with the OMNIA Partners team within first 90 days

As a continued partner of OMNIA Partners, Xerox's objective is to successfully implement the contract to ensure continued contract awareness, adoption and contract revenue growth. To achieve these goals, Xerox has developed a comprehensive 90-day action plan detailing how we will implement the contract upon award.

Within 30 days of award:

- Implement contract in the Xerox contract management system to enable order taking
- Create and distribute Press Release Announcement of Award
- Distribute Executive Sponsored Contract Award Announcement Communique to the Xerox Executive Leadership Teams and their respective sales and sales support resources, to include contract details, pricing and contract resource support
- Meet with OMNIA Partners Marketing team to develop specific co-marketing strategies to support the contract
- Created OMNIA Partners portal on Xerox.com

Within 60 days of award:

- Conduct contract training with all sales to highlight the benefits of our OMNIA Partners partner relationship, the scope of the contract, pricing, marketing strategies and available resources to support day to day sales activities
- Create co-marketing collaterals

Within 90 days of award:

- Assess success of contract launch and make adjustment as needed

B. Provide a detailed ninety-day plan beginning from award date of the Master Agreement describing the strategy to market the Master Agreement to current Participating Public Agencies, existing Public Agency customers of Supplier, as well as to prospective Public Agencies nationwide immediately upon award, to include, but not limited to:

i. Creation and distribution of a co-branded press release to trade publications

Xerox will work collaboratively with OMNIA Partners to create a press release to trade publications announcing the contract and highlighting the benefits of our continued partnership. We will amplify the great news through posts on Xerox's corporate social channels.

ii. Announcement, Master Agreements details and contact information published on the Supplier's website within first 90 days

Xerox Elite eCommerce Solutions can enable an OMNIA Partners' microsite for the online viewing of Xerox equipment, contract details, Xerox account team contact information and direct links to the OMNIA Partner's website. Xerox Elite eCommerce solutions can typically be launched within 30 days of contract award.

iii. Design, publication and distribution of co-branded marketing materials within first 90 days

Xerox will work in partnership with OMNIA Partners Marketing team to design and distribute co-branded marketing collateral for distribution to Xerox Sales, OMNIA Partner Region Managers and on-line retrieval.

iv. Commitment to attendance and participation with OMNIA Partners, Public Sector at national (i.e. NIGP Annual Forum, NPI Conference, etc.), regional (i.e. Regional NIGP Chapter Meetings, Regional Cooperative Summits, etc.) and supplier-specific trade shows, conferences and meetings throughout the term of the Master Agreement

Xerox attends and participates in many national, state and regional conferences throughout the year, such as NIGP, NAEP, CAPPO and more. Exhibit participation is dependent on current national, regional and local marketing funds.

v. Commitment to attend, exhibit and participate at the NIGP Annual Forum in an area reserved by OMNIA Partners, Public Sector for partner suppliers. Booth space will be purchased and staffed by Supplier. In addition, Supplier commits to provide reasonable assistance to the overall promotion and marketing efforts for the NIGP Annual Forum, as directed by OMNIA Partners, Public Sector.

Xerox understands the importance of attending and partnering with OMNIA Partners at the Public Sector NIGP Annual Forum. Xerox historically attends the NIGP Annual Form. Exhibit participation is dependent on current available marketing funds.

vi. Design and publication of national and regional advertising in trade publications throughout the term of the Master Agreement

Xerox does design and publish national/regional advertisements in trade publications. Participation is dependent upon current marketing funds and priorities.

vii. Ongoing marketing and promotion of the Master Agreement throughout its term (case studies, collateral pieces, presentations, promotions, etc.)

Xerox will work collaboratively with OMNIA Partners to develop a marketing plan to promote the use of the Master Agreement which may include case studies, co-branded collaterals, campaigns, etc.

viii. Dedicated OMNIA Partners internet web-based homepage on Supplier's website with:

- OMNIA Partners, Public Sector standard logo;
- Copy of original Request for Proposal;
- Copy of Master Agreement and amendments between Principal Procurement Agency and Supplier;
- Summary of Products and pricing;
- Marketing Materials
- Electronic link to OMNIA Partners, Public Sector's website including the online registration page;
- A dedicated toll-free number and email address for OMNIA Partners, Public Sector

Offered as a value added service to our clients, upon contract award, Xerox will provide OMNIA Partners with a dedicated private and custom web portal, branded with the OMNIA Partners standard logo, which will include the following information:

- Original RFP
- Master Agreement and amendments
- Summary of Products and pricing
- Xerox product documentation and marketing materials (specification sheets, brochures, YouTube videos)
- The OMNIA Partners, Public Sector toll-free number and email address
- Link to the OMNIA Partners, Public Sector website
- Xerox account team contact information

C. Describe how Supplier will transition any existing Public Agency customers' accounts to the Master Agreement available nationally through OMNIA Partners, Public Sector. Include a list of current cooperative contracts (regional and national) Supplier hold and describe how the Master Agreement will be positioned among other cooperative agreements.

Xerox has hundreds of state and local government contracts within the US which, per state law, allow for cooperative purchasing. Listed below are the actual national cooperative group purchasing contracts that Xerox is currently awarded on. Within an active procurement cycle, we provide the contract based on the needs, requirements and requests of the procurement agency. Within every procurement order, Xerox provides an implementation plan to allow for transparent transition from one contract to another.

Cooperative contracts include:

- OMNIA Partners
- GSA Schedule 70
- NASPO ValuePoint
- E&I
- PEPPM
- Sourcewell

D. Acknowledge Supplier agrees to provide its (logo(s) to OMNIA Partners and agrees to provide permission for reproduction of such logo in marketing communications and promotions. Acknowledge that use of OMNIA Partners logo will require permission for reproduction, as well.

Because of the tremendous value associated with our brand, Xerox provides our company logo after the review of the use of our logo by the Xerox brand team, prior to the release of any marketing communications. Xerox Corporation shall have ten business days to approve such use prior to publication. Any use of OMNIA Partners Public Sector name and logo or any form of publicity, inclusive of press releases will have prior approval from OMNIA Partner.

E. Confirm Supplier will be proactive in direct sales of Supplier's goods and services to Public Agencies nationwide and the timely follow up to leads established by OMNIA Partners, Public Sector. All sales materials are to use the OMNIA Partners, Public Sector logo. At a minimum, the Supplier's sales initiatives should communicate:

- i Master Agreement was competitively solicited and publicly awarded by a Principal Procurement Agency
- ii Best government pricing
- iii No cost to participate
- iv Non-exclusive

Xerox acknowledges and agrees.

F. Confirm Supplier will train its national sales force on the Master Agreement. At a minimum, sales training should include:

- i. Key features of Master Agreement
- ii. Working knowledge of the solicitation process
- iii. Awareness of the range of Public Agencies that can utilize the Master Agreement through OMNIA Partners, Public Sector
- iv. Knowledge of benefits of the use of cooperative contracts

Xerox acknowledges and agrees.

G. Provide the name, title, email and phone number for the person(s), who will be responsible for:

i. Executive Support

Mark Browning | Vice President

Public Sector / Healthcare Center of Excellence

Sales Enablement Americas Operations

mark.browning@xerox.com

Phone: 717-777-6624

ii. Marketing

Staci McKee | Global Integrated Marketing

Government | Healthcare | Education

Staci.mckee@xerox.com

Phone: 303-881-3718

iii. Sales

Rachael Jones Turner | SLED Cooperative Contracts Manager

Public Sector / Healthcare Center of Excellence

Sales Enablement Americas Operations

Rachael.Jones@Xerox.com

Phone: 310-258-6266

[iv. Sales Support](#)

Jennifer Melgar | S&L Cooperative Contract Support Administrator

NAO – SE Xerox Sales Support Center

Jennifer.Melgar@Xerox.com

Phone: 503-685-2239

[v. Financial Reporting](#)

Kathlene M. Andris | Rebate Analyst

US Customer Business Operations

Kathlene.Andris@Xerox.com

Phone: 847-928-2543

[vi. Accounts Payable](#)

Kevin Rowland | Accounts Payable Manager | Systems Support Manager

CFO Global Operations

Kevin.Rowland@xerox.com

Phone: 585-427-3974

[vii. Contracts](#)

Rachael Jones Turner | SLED Cooperative Contracts Manager

Public Sector / Healthcare Center of Excellence

Sales Enablement Americas Operations

Rachael.Jones@Xerox.com

Phone: 310-258-6266

[H. Describe in detail how Supplier's national sales force is structured, including contact information for the highest-level executive in charge of the sales team.](#)

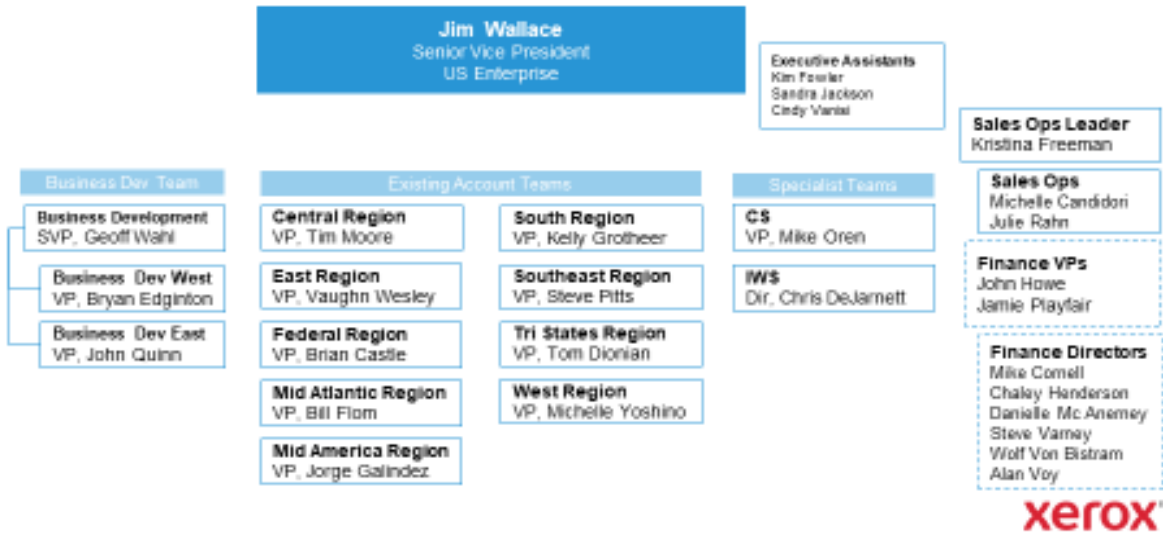
Go To Market Teams

Xerox is organized from a sales perspective on the basis of “go-to-market” sales channels. These sales channels are structured to serve a range of customers for our products and services.

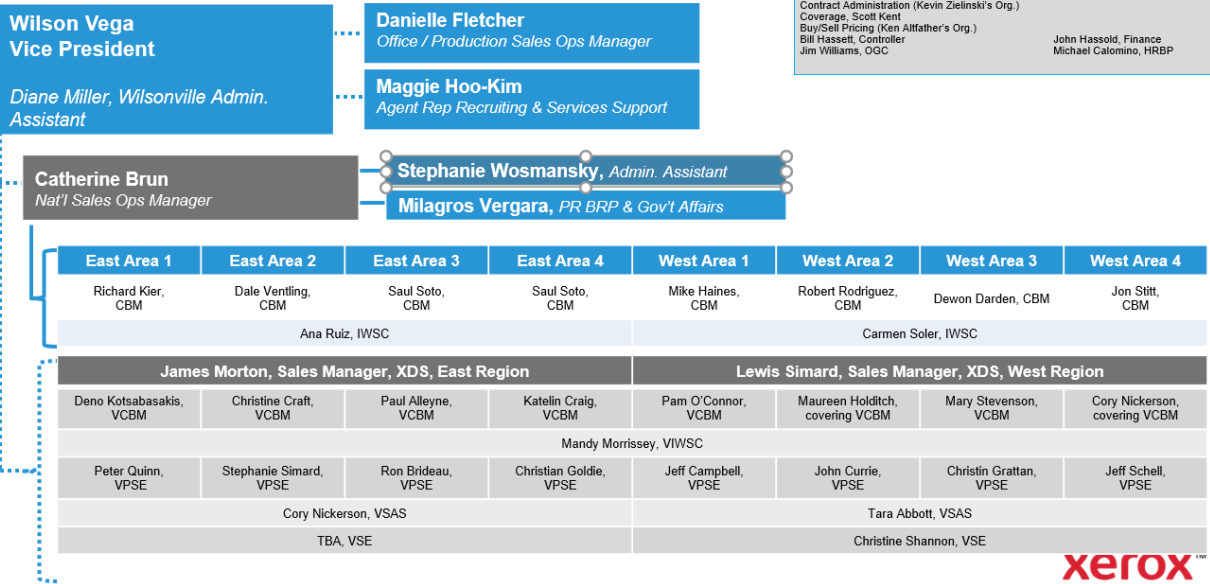
- **Mike Feldman**, President of the Americas Operations for Xerox Corporation, leads the company's go-to-market teams in the U.S., Canada, Mexico, Central and South America. Our sales go-to-market teams are focused on bringing our full portfolio or product offerings to current and new customers and partners, while maximizing and expanding coverage through direct and indirect channels.
- **Jim Wallace** leads both the U.S. Commercial Named Accounts and the Government, Healthcare & Education (GHE) sales teams.
- **Wilson Vega** leads the U.S. Agents, Xerox authorized independent agents.
- **Joanne Collins Smee**, the Xerox Chief Commercial Officer, is the Interim XBS President leading our wholly owned subsidiary, Xerox Business Services (XBS) - formerly known as Global Imaging Systems), an office technology dealer comprised of regional companies in the U.S.

US Enterprise Organization Chart

March 2020



US Agent Operations Organization Chart



Joanne Collins Smee
Xerox Chief Commercial Officer
Interim XBS President
Joanne.Collins@xerox.com
 (203) 849-2389

XBS SLT Direct Reports



Shelly Jacob, Executive Assistant 813.960.5508 x20224

 Bob Leone (808) 775-6332 Bob.Leone@xerox.com	 Wilson Vega (980) 305-8074 wvega@xbs-gis.com	 Ralph Söder (844) 800-2783 Ralph.Soder@xerox.com	 Sylvia Carrizosa VP, Sales Operations & Marketing 813.326.7698 Office 717.421.8853 Cell
<p>MRC/GOC, ISS, ZIG, Hawaii</p>	<p>GAR, CBS, GDS, COT/MDTO, ITS, STW Services Executive</p>	<p>CGS, GS, IOT, IOL, LDW, NEM, MQS, RKD Production Executive</p>	<ul style="list-style-type: none"> Sales Coverage & Sales Operations Direct & Agent Channel Mkt Transfer & Merge Sales & Analyst Product/Technology Skill Development Field Marketing Skill Development Sales & Analyst Support Infrastructure Production & Software Solutions Business Growth Product Portfolio Selection & Launch Marketing & Sales Management New Acquisition Sales Due Diligence & Integration Corporate Communications
 Brad Rollins (714) 569-1986 Brad@xbs@xerox.com	 George Cavaliaro (313) 633-4004 gcavali@xerox.com	Joanne Collins Smee Joanne.Collins@xerox.com (203) 849-2389	
<p>XBS SW (DAH, DEN, GDS & ASB) DocuShare & XMPi Executive</p>	<p>XBS SE (BER, STO, SDPL, SAK, ZDS)</p>	<p>AMC, ADT, BOE & NWO</p>	

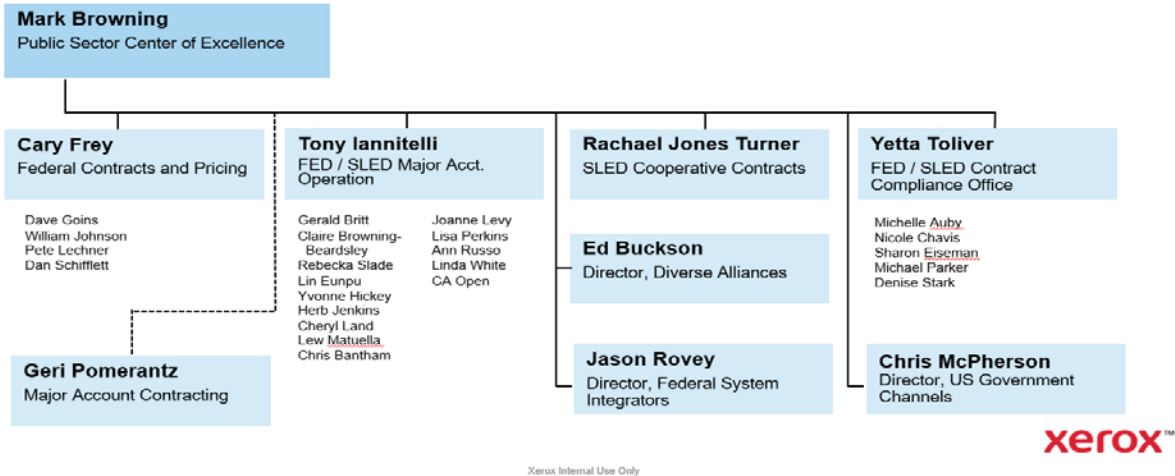


Public Sector / Healthcare Center of Excellence

On January 1, 2014, Xerox established a Public Sector Center of Excellence (COE), led by Mark Browning. The COE is responsible for the successful implementation and results stemming from the implementation of Federal, State & Local, Education and Healthcare contracts. The COE is focused on all aspects of contract support:

- Enabling the contracting for Federal, State, Local, Education and Healthcare contracts.
- Fostering high level executive relationships across the Federal and SLED markets.
- Drive strategic opportunities in both Technology and Managed Print Services to accelerate revenue growth.
- Provide consistent support across all Xerox sales channels.
- Contract Management to provide timely contract reports/fees payment.
- Manage contract compliance issues and audit readiness.

Public Sector Center of Excellence



Rachael Jones Turner is the US Director, SLED Cooperative Contract, providing strategic direction and deployment of Cooperative contracts in all Xerox Sales Channels across North America. She provides ongoing support, training and national implementation.

I Explain in detail how the sales teams will work with the OMNIA Partners team to implement, grow and service the national program.

We have found positive results in taking a collaborative approach with OMNIA Partners to market our contract to public agencies to drive both awareness and adoption. We depend on our partner's willingness and support to help carry our message and promote our technology and we have learned that taking a joint approach for these initiatives often yields higher rates of success in the long-term. We encourage sales integration to strategize on account specific opportunities, bridge relationships between the member and Xerox and support customer eligibility questions. During the training and launch of the contract, Xerox will reinforce the role of the OMNIA Partner's Region Managers and will encourage integration during Xerox sales team meetings and one-on-one interaction for account specific opportunities.

J. Explain in detail how Supplier will manage the overall national program throughout the term of the Master Agreement, including ongoing coordination of marketing and sales efforts, timely new Participating Public Agency account set-up, timely contract administration, etc.

Xerox will continue managing the national program throughout the term of the contract by leveraging our superior national infrastructure solely responsible for all aspects of government contracting. The Xerox Public Sector Center of Excellence (COE) ensures contract education nationally, consistency of pricing and controls, compliance to the terms and conditions of the contract, sales reporting and marketing and sales efforts. Within the COE, we have dedicated resources who are responsible for managing each core competency. Throughout the term of the master agreement, this team will lead the efforts to coordinate all aspects of the management of the contract.

K. State the amount of Supplier's Public Agency sales for the previous fiscal year. Provide a list of Supplier's top 10 Public Agency customers, the total purchases for each for the previous fiscal year along with a key contact for each.

Xerox does not make this information publicly available. A significant portion of our revenues is derived from contracts with U.S. state and local governments and their agencies.

L. Describe Supplier's information systems capabilities and limitations regarding order management through receipt of payment, including description of multiple platforms that may be used for any of these functions.

Orders are entered into a centralized ordering system which is accessible to only authorized Sales Representatives and the Order Processing Representatives. Editing of the order is completed and the request for equipment or service is passed to distribution in the equipment procurement system to establish a delivery date and time. Additionally, any special requirements are noted, and the appropriate departments are automatically notified if their involvement is necessary at the time of installation. Once successfully installed and accepted a notification is sent to the billing system to start the invoicing of the equipment or service. Invoices are generated and delivered to the customer and are due upon receipt. Generally, any equipment ordered or invoiced can be tracked and any needed reporting can be pulled from a centralized database.

M. If the Supplier wants to guarantee sales, provide the Contract Sales (as defined in Section 10 of the National Intergovernmental Purchasing Alliance Company Administration Agreement) that Supplier will guarantee each year under the Master Agreement for the initial three years of the Master Agreement ("Guaranteed Contract Sales").

\$ _____ .00 in year one

\$ _____ .00 in year two

\$ _____ .00 in year three

To the extent Supplier guarantees minimum Contract Sales, the administration fee shall be calculated based on the greater of the actual Contract Sales and the Guaranteed Contract Sales.

Xerox does not guarantee minimum contract sales as we are not familiar with the participating public agencies that are anticipated to utilize the resulting Master Agreement. Xerox will pay 3% on all revenue billed under the contract.

N. Even though it is anticipated many Public Agencies will be able to utilize the Master Agreement without further formal solicitation, there may be circumstances where Public Agencies will issue their own solicitations. The following options are available when responding to a solicitation for Products covered under the Master Agreement.

i. Respond with Master Agreement pricing (Contract Sales reported to OMNIA Partners).

ii. If competitive conditions require pricing lower than the standard Master Agreement not-to-exceed pricing, Supplier may respond with lower pricing through the Master Agreement. If Supplier is awarded the contract, the sales are reported as Contract Sales to OMNIA Partners under the Master Agreement.

iii. Respond with pricing higher than Master Agreement only in the unlikely event that the Public Agency refuses to utilize Master Agreement (Contract Sales are not reported to OMNIA Partners).

iv. If alternative or multiple proposals are permitted, respond with pricing higher than Master Agreement, and include Master Agreement as the alternate or additional proposal.

Detail Supplier's strategies under these options when responding to a solicitation.

Applicable to all four of these situations, whether a formal solicitation or not, as Xerox is requested to participate in a procurement cycle with an OMNIA Partner member, we will provide unique pricing equal to or below the not to exceed pricing based on bulk buy provisions per the terms and conditions of the University of California Master Agreement. If the individual procuring agency requires us to amend those terms and conditions to meet their specific state laws or requirements, we will provide an addendum in conjunction with the master terms and all revenue will be reported under OMNIA Partners.

COMPANY / GROUP	STREET ADDRESS	CITY/STATE/ZIP	WEB ADDRESS	SALES MGR/VP
Xerox Business Solutions, Inc.	8701 Florida Mining Blvd	Tampa, FL 33634	www.xerobusinesssolutions.com	Sylvia Carrizosa
Amcom Office - AMC	3600 McClaren Woods Drive	Coraopolis, PA 15108	www.teamamcom.com	David Saber
Arizona Office Technologies - AOT	4320 E. Cotton Center Blvd #100	Phoenix, AZ 85040	www.aot-xerox.com	David Hague
Berney Office Solutions - BER	10690 John Knight Close	Montgomery, AL 36117	www.berney.com	David Washington
Berney Office Solutions - BER	780 Lakeside Drive W., Ste B	Mobile, AL 36693	www.berney.com	David Washington
Berney Office Solutions - BER	4970 Corporate Drive, Ste 125H	Huntsville, AL 35805	www.berney.com	David Washington
Stewart of Alabama, Inc. - STO	4000 Colonnade Parkway	Birmingham, AL 35243	www.berney.com	Matt Fulmer
Carr Business Systems - CAR	500 Commack Road, Ste 110	Commack, NY 11725	www.carrxerox.com	Joe Savino
Carr Business Systems - CAR	485 Lexington Ave FL25	New York, NY 10017	www.carrxerox.com	Joe Savino
Connecticut Bus. Systems - CBS	100 Great Meadow Rd	Wethersfield, CT 06109	www.cbs-gisx.com	Steve Velardi
Connecticut Bus. Systems - CBS (Warehouse)	240 Pane Rd	Newington, CT 06111	www.cbs-gisx.com	Steve Velardi
Connecticut Bus. Systems - CBS	134 Capital Drive	West Springfield, MA 01089	www.cbs-gisx.com	Joe Cunningham
Connecticut Bus. Systems - CBS	465 Taylor Street	Springfield, MA 01105	www.cbs-gisx.com	Joe Cunningham
Connecticut Bus. Systems - CBS	931 Jefferson Blvd	Warwick, RI 02886	www.cbs-gisx.com	Joe Cunningham
Integrity One Technologies, Inc.- IOT	2920 Fortune Circle W, Suite C	Indianapolis, IN 46241	www.iot-xerox.com	Steve Shank
Integrity One Technologies, Inc.- IOT	801 N Capitol Avenue	Indianapolis, IN 46204	www.iot-xerox.com	Steve Shank
Integrity One Technologies, Inc.- IOT	2120 High Wickham Place	Louisville, KY 40245	www.iot-xerox.com	Stephanie Maloney
ComDoc, Inc. - COM	8247 Pittsburg Avenue NW	North Canton, OH 44720	www.comdoc.com	Keith Hanawalt
ComDoc, Inc. - COM	9100 South Hills Blvd. (Cleveland)	Broadview Hgts, OH 44147	www.comdoc.com	Tony Rugar
ComDoc, Inc. - COM	9999 Carver Road, Ste 100	Blue Ash, OH 45242	www.comdoc.com	Tim Combs
ComDoc, Inc. - COM	330 West Spring St, Ste 100 & 140	Columbus, OH 43215	www.comdoc.com	David Cathers
ComDoc, Inc. - COM (Warehouse)	711-713 Hadley Drive (WH)	Columbus, OH 43228	www.comdoc.com	David Cathers
ComDoc, Inc. - COM	55 Amherst Villa Rd	Buffalo, NY 14225	www.comdoc.com	Eric Smith
Capital Busines Systems, Inc.- CBU	2708 Commerce Drive, Unit A	Harrisburg, PA 17110	www.capitalbusinessinc.com	David Schlomer
Conway Technology Group LLC - COP	10 Capitol Street	Nashua, NH 03063	www.conwayoffice.com	Carl Tourigny
Conway Tech Group LLC - COP d/b/a Transco	34 Leighton Road	Augusta, ME 04330	www.transcobusiness.com	David Palmer
Conway Tech Group LLC - COP d/b/a BEU	275 Read Street	Portland, ME 04103	www.beu.net	David Palmer
Capitol Office Solutions, LLC - COS	9065 Guilford Road	Columbia, MD 21046	www.cosxs.com	MIF Specialist
Chicago Office Technology Group, Inc. - COTG	3 Territorial Court	Bolingbrook, IL 60440	www.cotg.com	Brian McCullough
Chicago Office Technology Group, Inc. - COTG	1 East Wacker Dr, #1305	Chicago, IL 60601	www.cotg.com	Brian McCullough

Chicago Office Technology Group, Inc. - COTG

Two Pierce Pl, Ste 12th Floor

Itasca, IL 60143

www.cotg.com

Brian McCullough

Carolina Office Systems - CSS

10506 Bryton Corp Center Dr, Ste 400

Huntersville, NC 28078

www.carolinaos.com

Brad Kikendall

Carolina Office Systems - CSS

2265 Clements Ferry Rd, Ste 203

Charleston, SC 29492

www.carolinaos.com

Brad Kikendall

G-Five, Inc. - GFI

297 Garlington Rd, Suite H

Greenville, SC 29615

www.gfive.net

Justin Wagner

Dahill Office Technology Corp-DAH d/b/a Xerox Business Solutions Southwest	8200 IH 10 W, Suite 400	San Antonio, TX 78230	www.dahill.com	Bonnie Garza
Dahill Office Technology Corp-DAH d/b/a Xerox Business Solutions Southwest	17280 Green Mtn Road, Ste. 130	San Antonio, TX 78247	www.dahill.com	Bonnie Garza
Dahill Office Technology Corp-DAH d/b/a Xerox Business Solutions Southwest	2100 West Loop South, Ste 1300	Houston, TX 77027 (Galleria)	www.dahill.com	Bonnie Garza
Dahill Office Technology Corp-DAH d/b/a Xerox Business Solutions Southwest	5747 Brittmoore Rd, Suite 100	Houston, TX 77041 (WH)	www.dahill.com	Bonnie Garza
Dahill Office Technology Corp-DAH d/b/a Xerox Business Solutions Southwest	901 S. Mopac Expwy, Ste 595	Austin, TX 78746	www.dahill.com	Bonnie Garza
Dahill Office Technology Corp-DAH d/b/a Xerox Business Solutions Southwest	11831 Miriam, Unit A-9 (Serv Wh)	El Paso, TX 79936		Bonnie Garza
Denitech Corporation - DEN	820 W Sandy Lake Rd, Ste 100	Coppell, TX 75019	www.denitech.com	Bonnie Garza
Dahill Office Technology Corp-DAH d/b/a Xerox Business Solutions Southwest	100 North Mustang Rd. Dock 1	Yukon, OK 73099	www.youronesource.com	Thomas Meagher
Eastern Managed Print Network - ECP	1224 W. Genessee St.	Syracuse, NY 13204	www.easternmpn.com	Steve Wilmarth
Eastern Managed Print Network - ECP	111 Grant Avenue	Endicott, NY 13760	www.easternmpn.com	Steve Wilmarth
Eastern Managed Print Network	8 Access Road	Colonie (Albany), NY 12205	www.easternmpn.com	Steve Wilmarth
Elan Marketing, Inc. d/b/a Elan Office Systems	6760 Surrey Street	Las Vegas, NV 89119	www.elanoffice.com	John Gallegos
Electronic Systems - ESI	369 Edwin Drive (Building 1)	Virginia Beach, VA 23462	www.esi.net	Steve Pitts
Electronic Systems - ESI	365 Edwin Dr (Bldg. 2-not publishd)	Virginia Beach, VA 23462	www.esi.net	Steve Pitts
Electronic Systems - ESI	4417 Expressway Dr	Virginia Beach, VA 23452	www.esi.net	Steve Pitts
Electronic Systems - ESI	3727 Challenger Avenue	Roanoke, VA 24012	www.esi.net	Steve Pitts
Electronic Systems - ESI	10406 Lakeridge Parkwy, Ste 1000	Ashland, VA 23055	www.esi.net	Steve Pitts
TML Enterprises, Inc. - TML	4151 Lafayette Center Dr, Ste 100	Chantilly, VA 20151	www.tml-xerox.com	Steve Pitts
GDP Technologies, Inc. - GDP	1180 Eisenhower Parkway	Macon, GA 31206	www.gadup.com	Keith Harper
GDP Technologies, Inc. - GDP	4350 Rivergreen Parkway, Ste 100	Duluth, GA 30096	www.gadup.com	Keith Harper
imageQuest - IQI	11021 E 26th Street N	Wichita, KS 67226	www.imagequestks.com	Paul Morton
imageQuest - IQI	11106 Strang Line Rd, Bldg K	Lenexa, KS 66213	www.imagequestks.com	Paul Morton
Image Technology Specialists, Inc. - ITS	70 Shawmut Road	Canton, MA 02021	www.its-xrx.com	Randy Baril
Lewan & Associates - LEW	1400 South Colorado Blvd.	Denver, CO 80222	www.lewan.com	Michael Carroll
Lewan & Associates - LEW (Warehouse)	8530 Concord Center Dr, #400	Englewood, CO 80112	www.lewan.com	Michael Carroll
Lewan & Associates - LEW	1551-D Mercantile Avenue NE	Albuquerque, NM 87107	www.lewan.com	Michael Carroll
LRI, LLC	1601 SE Gateway Drive, Ste 130	Grimes, Iowa 50111	www.laserresources.com	Paul Bronke
Merizon Group, Inc - MBM Business Machines	d/b/a Modern 620 N. Lynndale Drive	Appleton, WI 54914	www.mbm360.com	Jason Loker
Michigan Office Solutions - MOS	2859 Walkent Drive NW	Grand Rapids, MI 49544	www.mos-xerox.com	Keith Stewart
Michigan Office Solutions - MOS	3101 Technology Blvd, Ste J	Lansing, MI 48910	www.mos-xerox.com	Keith Stewart
Michigan Office Solutions - MOS	40000 Grand River, Ste 500	Novi, MI 48375	www.mos-xerox.com	Walter Reynolds

Minnesota Office Technology Group - MOTG

5600 Rowland Rd, Ste 205

Minnetonka, MN 55343

www.motg-xerox.com

Christopher Reeves

Mr. Copy, Inc. - MRC, d/b/a MRC Smart Technology Solutions	5657 Copley Dr.	San Diego, CA 92111	www.mrc360.com	Charlie Sinnen
Mr. Copy, Inc. (Warehouse)	5625-5629 Copley Dr	San Diego, CA 92111	www.mrc360.com	Charlie Sinnen
Mr. Copy, Inc. - MRC, d/b/a MRC Smart Technology Solutions	5050 Hopyard Road, Ste 100	Pleasanton, CA 94588	www.mrc360.com	Charlie Sinnen
Mr. Copy, Inc. - MRC, d/b/a MRC Smart Technology Solutions	(Waref 21343 Cabot Blvd, Bldg A	Hayward, CA 94545	www.mrc360.com	Charlie Sinnen
Rabbit Office Automation (ROA)	904 Weddell Court	Sunnyvale, CA 94089	www.roa-usa.com	Charlie Sinnen
Inland Business Systems, Inc. - IBS	1326 N. Market Blvd,	Sacramento, CA 95834	www.iqinland.com	Bill Mello
Inland Business Systems, Inc. - IBS aka Sierra Office Solutions - SIO	4710 Longley Lane	Reno, NV 89502	www.sierraoffice.com	Bill Mello
Inland Business Systems, Inc. - IBS aka Lucas Business Systems, Inc. - LUC	627 Bitritto Court	Modesto, CA 95351	www.lucassystems.com	Bill Mello
Inland Business Systems, Inc. - IBS aka Lucas Business Systems, Inc. - LUC	2592 Notre Dame Blv	Chico, CA 95928	www.lucassystems.com	Bill Mello
SoCal Office Technologies f/d/b/a MWB Copy Products. - SOC	5700 Warland Drive	Cypress, CA 90630	www.socal-office.com	Stephanie Bannon
Zoom Imaging Solutions - ZIS	4603 W. Jennifer Ave.	Fresno, CA 93722	www.zoomcopiers.com	Charlie Sinnen
Xerox Hawaii - XHI	700 Bishop Street, Ste 1200	Honolulu, HI	www.xerox.com	Ian Yee
MT Business Technologies, Inc. - MTB	1150 National Parkway	Mansfield, OH 44906	www.mtbt.com	Mark Oswald
MT Business Technologies, Inc. - MTB	1205 Corporate Drive	Holland, OH 43528	www.mtbt.com	Mark Oswald
Quality Business Systems - QBS	14432 SE Eastgate Way, Ste 300	Bellevue, WA 98007	www.qbsi-xerox.com	Paul Franetovich
Quality Business Systems - QBS (Warehouse)	7112 S. 212th Street	Kent, WA 98032	www.qbsi-xerox.com	Paul Franetovich
CTX Business Solutions d/b/a Copytronix - CTX	16640 SW 72nd Ave, Bldg 10	Portland, OR 97224	www.ctx-xerox.com	Kyle Marvin
Boise Office Equipment, Inc. - BOE	330 North Ancestor Place	Boise, ID 83704	www.boeweb.com	Rob Davis
R.K. Dixon Company - RDK	5700 Utica Ridge Road	Davenport, IA 52807	www.rkdixon.com	Paul Bronke
R.K. Dixon Company - RDK	8630 North Allen Road	Peoria, IL 61615	www.rkdixon.com	Nick Barnes
Premier Office Equipment, Inc. - POE	1510 East Olive Street	Marshalltown, IA 50158	www.premierofficeequipment.com	Nick Barnes
Saxon Business Systems - SAX	14025 NW 60th Avenue	Miami Lakes, FL 33014	www.saxon.net	Bert LaCalle
Saxon Business Systems - SAX	1395 NW 17th Avenue, #107	Delray Beach, FL 33445	www.saxon.net	Bert LaCalle
Saxon Business Systems - SAX	9150 Phillips Highway, Ste 2	Jacksonville, FL 32256	www.saxon.net	Bert LaCalle
Stewart Business Systems - STW	6000 Irwin Road, Suite A	Mt. Laurel, NJ 08054	www.stewartxerox.com	Kathy DiMaggio
Stewart Business Systems - STW (Warehouse)	3001 Irwin Road, Suite B&C	Mt. Laurel, NJ 08054	www.stewartxerox.com	Kathy DiMaggio
Stewart Business Systems - STW	365 W. Passaic St, Ste 585	Rochelle Park, PA 07662	www.stewartxerox.com	Kathy DiMaggio
Zeno Office Solutions - ZOS	8701 Florida Mining Blvd	Tampa, FL 33634	www.zenosolutions.com	Bill Batrow

Xerox Authorized Sales Agents

Establishment	Owner_First	Owner_Last	Address1	City	State	Zip
ADVANCED XEROGRAPHICS	RAYMOND	BURT	307 S. MAIN STREET	UKIAH	CA	95482
SMART DOCUMENT SOLUTIONS - (LAKE HAVASU)	TRACEY	ARVIEUX	4045 E. PALM LANE	PHOENIX	AZ	85008
COPIERS PLUS INC	KRIS	SMITH	218 NORTH MAIN, SUITE 1	MONTICELLO	IN	47960
NORTHEAST OFFICE EQUIPMENT	JIM	CHIACCHIERO	1520 W. 13TH STREET	ASHTABULA	OH	44004
PENDRED OFFICE MACHINES	MICHAEL	PENDRED	1233 N. MISSION	MT. PLEASANT	MI	48858
DIGITAL DOCUMENT SOLUTIONS	LANNY	LEONARD	324 NO. MCPHERSON CHURCH ROAD - 2ND FL	FAYETTEVILLE	NC	28303
AMERICAN BUSINESS CENTER MPS, INC.	RICHARD	YEATS	PO BOX 20128	PANAMA CITY	FL	32417
DOCUGRAPHICS, LLC	THOMAS	FIMIAN	6624-C GORDON ROAD	WILMINGTON	NC	28411
COPIERS ETC.	PEGGY ANN	BRANNON	148 SOUTH DOROUGH ROAD	CORDELE	GA	31015
XDOS, INC.	HAROLD	NIXON	18 EAST LIBERTY STREET	SUMTER	SC	29150
ADVANTAGE BUSINESS PRODUCTS	RANDY	KIDWELL	2064 S. WESTERN AVENUE	SPRINGFIELD	MO	65807
PROFESSIONAL OFFICE PRODUCTS, INC. (II)	JASON	MONTET	441 N. MAIN	JENNINGS	LA	70546
JUSTTECH, LLC (VI)	JOSHUA	JUSTICE	101 CATALPA DR STE #102	LA PLATA	MD	20646
QUALITY QUICKLY	BRIAN	MARSHALL	945 3rd AVE SE SUITE 103	HICKORY	NC	28602
RYDER BROTHERS STATIONERY	RANDY	DODSON	1735 MAIN STREET	BAKER CITY	OR	97814
BUSINESS EQUIPMENT LLC	MARK	DURBIN	PO BOX 7948	PADUCAH	KY	42003
BUSINESS IMPRESSIONS	JEFF	BASSETT	PO BOX 959	AUBURN	IN	46706
BUTLER'S OFFICE EQUIPMENT & SUPPLY (EAST)	PATRICK	BUTLER	1900 E. HISTORIC HWY 66, SUITE C	GALLUP	NM	87301
BENCHMARK BUSINESS SOLUTIONS, INC. (NEW MEXICO)	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
XEROGRAPHIC EQUIPMENT SYSTEMS	MICHAEL	MCKENNA	PO BOX 794	CHEYENNE	WY	82003
METRO CENTRE, LP	KARLA	METZLER	679 COUNTY ROAD 404	GAINESVILLE	TX	76240
BEST OFFICE SOLUTIONS	BOB	VALENTA	PO BOX 849	ATLANTA	TX	75551
COMPUTERS911, LLC (II)	BILLY	TINGLE	403 N. MAIN	MARKSVILLE	LA	71351
COMPUTERS911, LLC	BILLY	TINGLE	403 N. MAIN	MARKSVILLE	LA	71351
X WEST INC.	RANDALL	BERNHARDT	12136 W. BAYAUD AVE., STE 125	LAKESWOOD	CO	80228
PROFESSIONAL OFFICE PRODUCTS, INC. (III)	JASON	MONTET	441 N. MAIN	JENNINGS	LA	70546
SOUTH TEXAS SALES	SONNY	HOELSCHER	1901 EAST MAIN STREET	ALICE	TX	78332
ALABAMA OFFICE SUPPLY	HARRIS	ASBURY	PO BOX 467	OPELIKA	AL	36801
COLONY OFFICE PRODUCTS	DAN	WILSON	121 EAST WASHINGTON STREET	DEMOPOLIS	AL	36732
LOW COUNTRY OFFICE SOLUTIONS	DON	NESBITT	802 EAST MARTINTOWN RD, SUITE 162	NO. AUGUSTA	SC	29841
SOUTHERN OFFICE EQUIPMENT, LLC	TIMOTH	TODD	PO BOX 636	DAPHNE	AL	36526
NO MISSISSIPPI BUS PRODUCTS	MARK	FOSTER	223 SHARKEY AVE., SUITE 104	CLARKSDALE	MS	38614
MICKEY MAYS OFFICE SOLUTIONS	MICKEY	MAYS	600 MONROVIA DR	RUSTON	LA	71270
PREFERRED OFFICE MACHINES	JOHN	MILAN	215 NORTH MICHIGAN	BIG RAPIDS	MI	49307
DIGITAL OFFICE CENTRE	TOM	ROSTVEDT	515 20TH AVENUE SE, STE 11	MINOT	ND	58701
JUSTTECH, LLC (V)	JOSHUA	JUSTICE	101 CATALPA DR STE #102	LA PLATA	MD	20646
IMAGE MAKERS INC	LAURA	NYQUIST	3588 VETERANS DRIVE, SUITE 3	TRAVERSE CITY	MI	49684

VALLEY OFFICE PRODUCTS	LARRY	CANTINE	110 SOUTH MAIN STREET	MILBANK	SD	57252
THE BUSINESS CONNECTION	JAMES	PUCHNER	214 MAIN	CHADRON	NE	69337
PROFESSIONAL BUS PRODUCTS	KEN	MCBRIDE	PO BOX 1154	CRAB ORCHARD	WV	25827
ATLAS REPRODUCTION, INC.	MICHAEL	MCKENNA	PO BOX 2901	CASPER	WY	82601
XEROGRAPHIX EAST TEXAS	SCOTT	WALLER	424 NORTH STREET	NACOGDOCHES	TX	75961
SOUTHWEST OFFICE SOLUTIONS, INC. (BELEN)	TRACY	ASHTON	1789 CENTRAL AVENUE, SUITE 4	LOS ALAMOS	NM	87544
SUPERIOR OFFICE PRODUCTS	RANDY	POCHE	533 HIGHLANDIA DRIVE, STE K	BATON ROUGE	LA	70810
DOCUMENT SOLUTIONS (II)	LOREN	MAUK	1540 RICE ROAD, SUITE 100	TYLER	TX	75703
BUTLER'S OFFICE EQUIPMENT & SUPPLY (NORTH)	PATRICK	BUTLER	1900 E. HISTORIC HWY 66, SUITE C	GALLUP	NM	87301
PROFESSIONAL OFFICE PRODUCTS, INC.	JASON	MONTET	441 N. MAIN	JENNINGS	LA	70546
NORMAN ORR OFFICE SUPPLY, LLC	REID	GRIGSBY	202 WEST MAIN	WEST PLAINS	MO	65775
MERRIFIELD OFFICE SUPPLY, LLC	DARRELL	MERRIFIELD	224 SOUTH MAIN	ELK CITY	OK	73644
OFFICE EQUIPMENT SOURCE, INC. (II)	MIKE	MITCHELL	227 W. WATER STREET	ELMIRA	NY	14901
JUSTTECH, LLC (III)	JOSHUA	JUSTICE	101 CATALPA DR STE #102	LA PLATA	MD	20646
JUSTTECH, LLC (IV)	JOSHUA	JUSTICE	101 CATALPA DR STE #102	LA PLATA	MD	20646
WYTHEVILLE OFFICE SUPPLY	KENNETH WAYNE	ROOP	146 WEST MAIN STREET	WYTHEVILLE	VA	24382
COMPLETE DOCUMENT SOLUTIONS CENTRAL PENN LLC II	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
KYLE OFFICE SUPPLY	CHRIS	KYLE	1020 21ST AVENUE	TUSCALOOSA	AL	35401
COMPLETE DOCUMENT SOLUTIONS, MARYLAND LLC (IV)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
HUGHES OFFICE EQUIPMENT, LLC	JOHN	TURZIANO	PO BOX 278	BELLAIRE	OH	43906
SIERRA OFFICE SOLUTIONS	TODD	ALLRED	23811 WASHINGTON AVE STE C110-230	MURIETTA	CA	92562
PRINT 'N COPY CENTER	REECE	KEENER	565 W. SILVER ST.	ELKO	NV	89801
D-TECH NORTH, LLC	FRANK	DEFRANCESCO	1095 MILITARY TRL, UNIT 1447	JUPITER	FL	33458
BUDDE'S OFFICE SUPPLY	BERT	BUDDE	3210 FLAGLER AVENUE	KEY WEST	FL	33040
OFFICE AUTOMATION	DANIEL PATRICK	CURRIE	851 NW 250 TERRACE	NEWBERRY	FL	32669
PRECISION OFFICE SYSTEMS	ROBERT	DEMARCO	8817 NW 40th CIRCLE	GAINESVILLE	FL	32653
DOCUMENT SYSTEMS, INC. (II)	CRAIG	BRAME	89 MARKET STREET	HENDERSON	NC	27537
BUERGER OFFICE SYSTEMS	CAMERON	BUERGER	1670 WARREN ROAD	INDIANA	PA	15701
OFFICE EQUIPMENT SOURCE, INC. (I)	MIKE	MITCHELL	227 W. WATER STREET	ELMIRA	NY	14901
XEROGRAPHICS OF FLAGSTAFF, INC.	TRACEY	ARVIEUX	4045 E. PALM LANE	PHOENIX	AZ	85008
ADVANCED DOCUMENT SYSTEMS, INC.	HECTOR	LIZARDI	19226 66th AVE. S., SUITE L-100	KENT	WA	98032
DOCUMENT CONSULTING SERVICES	TED	SWICK	880 APOLLO STREET, SUITE 353	EL SEGUNDO	CA	90245
LAS AMERICAS OFFICE EQUIPMENT, INC.	FELIX	RIVERA	PO BOX 90	MERCEDITA	PR	00715
EXECUTIVE OFFICE EQUIPMENT	LAURANCE	BONELLI	PO BOX 6217	ST THOMAS	VI	00804
OFFITEK	FELIX	RIVERA	2980 EMILIO FAGOT AVENUE SUITE 2	PONCE	PR	00716
DOCUMENT COMPANY	JORGE	CANALS	AVE. LAUREL #GA11, CALLE 49, SANTA JUANITA	BAYAMON	PR	00956
C & M DOCUMENT COMPANY, INC.	JORGE	CANALS	MSC 848, AVENIDA WINSTON CHURHILL #138	SAN JUAN	PR	00926
COMPLETE DOCUMENT SOLUTIONS LLC (III)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
JUSTTECH, LLC (VII)	JOSHUA	JUSTICE	101 CATALPA DR STE #102	LA PLATA	MD	20646

ANNAPOLIS OFFICE PRODUCTS	JIM	SCHALGE	8258 VETERANS HIGHWAY, SUITE 3A	MILLERSVILLE	MD	21108
MARITIME BUSINESS CONCEPTS	SCOTT	WILLIAMS	1306 N. HERRITAGE ST	KINSTON	NC	28501
AMERICAN BUSINESS CENTER MPS INC. (II)	RICHARD	YEATS	PO BOX 20128	PANAMA CITY	FL	32417
OFFICE AUTOMATION (EAST-WEST)	DANIEL PATRICK	CURRIE	PO BOX 9	NEWBERRY	FL	32669
IMAGE SOURCE IV	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 540	SAN BERNARDINO	CA	92408
XEROGRAPHIC BUSINESS SYS	LARRY	GLEASON	819 WATER ST, SUITE 110.	KERRVILLE	TX	78028
XMC OF ARKANSAS	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
TALLAHASSEE TECHNOLOGY GROUP, INC.	RICHARD	MAUS	1949 RAYMOND DIEHL ROAD STE B	TALLAHASSEE	FL	32308
KIMBRELL'S DIGITAL SOLUTIONS	SCOTT	KIMBRELL	520 MAIN STREET	NATCHEZ	MS	39120
DOCUMENT SOLUTIONS EAST, INC.	DARRELL	HARRISON	PO BOX 4006	GREENVILLE	NC	27858
THE OFFICE ADVANTAGE	MARK	VAN DEN HOEK	318 N. MAIN	MITCHELL	SD	57301
FLYNN'S INC.	BRIAN	CANTOR	115 W 30th ST., RM 411	NEW YORK	NY	10001
T.E.C DOCUMENT SOLUTIONS	ANTHONY	GARCIA	231 WEST 29TH STREET SUITE 905	NEW YORK	NY	10001
DELMARVA DOCUMENT SOLUTIONS, INC.	JENNIFER	ATCHISON	112 SOUTH BOULEVARD	SALISBURY	MD	21804
DOCUMENT TECHNOLOGIES, INC.	JANICE	DUPLISEA	23 CROSBY DRIVE	BEDFORD	MA	01730
CSRA DOCUMENT SOLUTIONS	DON	NESBITT	802 EAST MARTINTOWN RD, SUITE 162	NO. AUGUSTA	SC	29841
IMAGE SOURCE	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 500	SAN BERNARDINO	CA	92408
PROFESSIONAL DOCUMENT SOLUTIONS, INC. (PDS - GJ)	TROY	TAFOYA	4114 TIMBERLINE ROAD	FORT COLLINS	CO	80525
UTOPIAN IQ SERVICES INC.	SEBASTIAN	MARTINEZ	6095 NW 82 AVE	MIAMI	FL	33166
IMPRESSIONS OF ASPEN, INC.	NANCY	TORINUS	P.O. BOX 295	CARBONDALE	CO	81623
ADVANCED DOCUMENT SOLUTIONS, INC. (II)	SCOTT	HAMILTON	819 S. FLOYD STREET	LOUISVILLE	KY	40203
TOTAL DOCUMENT SOLUTIONS, INC.	TIMOTHY	STANLEY	2515 NORTH SHILOH DRIVE	FAYETTEVILLE	AR	72704
COMPLETE DOCUMENT SOLUTIONS, NY LLC	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
XRX BUSINESS CONSULTANTS	DAVID	CAVAZOS	708 NORTH MCCOLL	MCALLEN	TX	78501
XMC OF MEMPHIS	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
XCEL OFFICE SOLUTIONS	MICHAEL	REID	304 N MERIDIAN AVE STE 18	OKLAHOMA CITY	OK	73107
DIXIE DIGITAL IMAGING, INC.	KELLY	SMITH	1401 COMMERCE COURT	FORT SMITH	AR	72908
SHAMROCK OFFICE SUPPLY	MIKE	FORMELLER	219 E. VEROT SCHOOL ROAD	LAFAYETTE	LA	70508
DOCUMENT SOLUTIONS OF SPRINGFIELD	GREG	TIGGES	1736 E. SUNSHINE STREET, SUITE 100	SPRINGFIELD	MO	65804
DOCUMENT SOLUTIONS, INC.	ROBERT	BIGHAM JR.	4401 N. MAIN ST., SUITE A	VICTORIA	TX	77904
BENCHMARK BUSINESS SOLUTIONS	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
COMPLETE OFFICE SOURCE INC.	GLEN	DUNN	429 CURWOOD DRIVE	OWOSSO	MI	48867
INDIANA BUSINESS SOLUTIONS	TIMOTHY	SLOPSEMA	8227 NORTHWEST BLVD., #200	INDIANAPOLIS	IN	46278
COPY SOLUTIONS, INC.	ROGER	ZHAO	919 S. FREMONT AVE, SUITE 398	ALHAMBRA	CA	91803
MORRIS COUNTY STATIONERS	RICHARD	FLETCHER	PO BOX 279	FLANDERS	NJ	07836
BENCHMARK BUSINESS SOLUTIONS, INC.-ABILENE	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
EDGE OFFICE PRODUCTS	LESTER	KILPATRICK	1909 JUDSON RD.	LONGVIEW	TX	75605
DOCUMENT SOLUTIONS	LOREN	MAUK	1540 RICE ROAD, SUITE 100	TYLER	TX	75703
COPIER CONNECTION	BONNIE	DOOLEY	10425 WESLEY	GREENVILLE	TX	75402

EXCEL OFFICE SERVICES	BRETT	BUTLER	12031 JEFFERSON BLVD	CULVER CITY	CA	90232
RAY BLOCK STATIONERY	GEORGE	GARCIA	3 PLAINFIELD AVE.	FLORAL PARK	NY	11001
XCL BUSINESS PRODUCTS	MICHAEL	DAVID	1767-46 VETERANS MEMORIAL HWY	ISLANDIA	NY	11749
OFFICE EVOLUTIONS, INC.	JOHN	GILLON	1808 WHEELER AVE STE #2	HOUSTON	TX	77004
ALASKA ENTERPRISE SOLUTIONS, INC. (FAIRBANKS)	MICHAEL	FERRIS	557 E FIREWEED LANE SUITE A	ANCHORAGE	AK	99503
HIGH COUNTRY COPIERS, INC.	TROY	TAFOYA	4114 TIMBERLINE ROAD	FORT COLLINS	CO	80525
KYLE OFFICE PRODUCTS	TOM	KYLE	418 TARROW	COLLEGE STATION	TX	77840
DOCUMENT SOLUTIONS (V)	LOREN	MAUK	1540 RICE ROAD, SUITE 100	TYLER	TX	75703
PREMIER OFFICE SYSTEMS	COLIN	MCTERNAN	500 N. RAINBOW BLVD. STE 312	LAS VEGAS	NV	89107
QUALITY BUSINESS	EDGARDO	RODRIGUEZ	1142 FD ROOSEVELT AVENUE	HATO REY	PR	00920
OFFICE EQUIPMENT SOURCE, INC. (VI)	MIKE	MITCHELL	227 W. WATER STREET	ELMIRA	NY	14901
PROFESSIONAL DOCUMENT SOLUTIONS (PDS)	TROY	TAFOYA	4114 TIMBERLINE ROAD	FORT COLLINS	CO	80525
IMAGE SOURCE - METRO	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 540	SAN BERNARDINO	CA	92408
IMAGE SOURCE - TEMECULA	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 540	SAN BERNARDINO	CA	92408
BENCHMARK OFFICE SYSTEMS INC.	MICHELLE	MCMANUS	75 GILCREAST RD., STE. 311	LONDONDERRY	NH	03053
ADVANCED DOCUMENT SOLUTIONS, INC. (III)	SCOTT	HAMILTON	819 S. FLOYD STREET	LOUISVILLE	KY	40203
DOCUMENT SOLUTIONS - TENNESSEE	KAREN	MCGINNIS	256 AVIGNON WAY	CLARKSVILLE	TN	37043
CONVERGING TECHNOLOGIES - SANTA ROSA	GENE	IRTENKAUF	4331 FISTOR DR	SANTA ROSA	CA	95409
ITECH	MICHAEL	WILLIAMS	326 5TH STREET	PARKERSBURG	WV	26101
NETWORK ENHANCEMENT SYSTEMS, INC.	EDGAR	SILKEY	10827 EAST MARSHALL STREET	TULSA	OK	74116
COMPLETE DOCUMENT SOLUTIONS	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
XCEL OFFICE SOLUTIONS, LLC	MICHAEL	REID	304 N MERIDIAN AVE STE 18	OKLAHOMA CITY	OK	73107
Q DOCUMENT SOLUTIONS	JOEL	HACKETT	3030 OLD RANCH PARKWAY, SUITE 190	SEAL BEACH	CA	90740
OFFICE TECH	B.K.	POWELL	3709 SPENARD ROAD SUITE 200	ANCHORAGE	AK	99503
TOTAL OFFICE SOLUTION OF WEST TEXAS	TOMMY	MCCRURY	1601 N. LEE AVENUE	ODESSA	TX	79761
DOCUMENT SYSTEMS	CRAIG	BRAME	89 MARKET STREET	HENDERSON	NC	27537
GREAT NORTHERN EQUIPMENT	KIM	BROWN	104 NE 3RD STREET, SUITE 200C	GRAND RAPIDS	MN	55744
COMPLETE DOCUMENT SOLUTIONS, NY LLC	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
WEST KENTUCKY XEROGRAPHICS LLC	JAMES	DEMA	PO BOX 124	BENTON	KY	42025
SOUTHERN DIGITAL LLC	ALBERT	HENRICKS	330 N JEFFERSON DAVIS PARKWAY	NEW ORLEANS	LA	70119
CONNEX SYSTEMS INC.	GREGORY	WALTER	2033 CHENAULT DR STE 150	CARROLLTON	TX	75006
IMAGE SOURCE (LA)	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 540	SAN BERNARDINO	CA	92408
PROFESSIONAL DOCUMENT SOLUTIONS, INC. (PDS – GJ II)	TROY	TAFOYA	4114 TIMBERLINE ROAD	FORT COLLINS	CO	80525
COPY CONNECTION	RAJAT	GANDHI	201 W. HILLSIDE, SUITE 24	LAREDO	TX	78041
ADVANCED XEROGRAPHY	DEREK	BARNES	1823 N. YELLOWWOOD	BROKEN ARROW	OK	74012
ADVANCED DIGITAL SOLUTIONS, INC	BILL	NORTHAM	1512 BROADWAY AVENUE	MATTOON	IL	61938
MOUNTAIN WEST OFFICE SOLUTIONS	BRUCE	PORCH	1205-B KENSINGTON AVENUE	MISSOULA	MT	59801
XDOS, INC.	HAROLD	NIXON	20 EAST LIBERTY STREET	SUMTER	SC	29150
DOCUMENT TECHNOLOGIES, INC. (SOUTH SHORE)	JANICE	DUPLISEA	23 CROSBY DRIVE	BEDFORD	MA	01730

AMBIZ SOLUTIONS, INC.	RICHARD	YEATS	PO BOX 20128	PANAMA CITY	FL	32417
SOUTHWEST OFFICE SOLUTIONS, INC. (LOS ALAMOS)	TRACY	ASHTON	1789 CENTRAL AVENUE, SUITE 4	LOS ALAMOS	NM	87544
WASATCH DOCUMENT SOLUTIONS INC.	CASEY	BECK	373 EDGEHILL DRIVE	PROVIDENCE	UT	84332
OFFICE SYSTEMS OF FAYETTE & GREENE	CAMERON	BUERGER	1670 WARREN ROAD	INDIANA	PA	15701
PDS DENVER TECH CENTER	TROY	TAFOYA	4114 TIMBERLINE ROAD	FORT COLLINS	CO	80525
DIGITAL OFFICE SOLUTIONS V	ROBERT	WEBB	4125 N. 124TH STREET, SUITE J	BROOKFIELD	WI	53005
MARCOTEK DIGITAL OFFICE SOLUTIONS II	KEITH	NORRIS	100 NORTH PATTERSON STREET	VALDOSTA	GA	31601
OFFICETECH NORTHWEST	B.K.	POWELL	6310 E. SPRAGUE AVENUE	SPOKANE	WA	99212
XEROGRAPHIC EQUIPMENT SYSTEMS - LARAMIE	MICHAEL	MCKENNA	PO BOX 794	CHEYENNE	WY	82003
IT BUSINESS SOLUTIONS	ROBERT	HAY	2698 CASSELMAN ROAD	ROCKWOOD	PA	15557
HEARTLAND DIGITAL IMAGING INC.	RYAN	VERCELLINO	6004 WILLOW SPRINGS	MARION	IL	62959
XMC OF LITTLE ROCK, INC.	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
OFFICE TECH - WENATCHEE	B.K.	POWELL	6310 E. SPRAGUE AVENUE	SPOKANE	WA	99212
DIGITAL OFFICE SOLUTIONS	ROBERT	WEBB	4125 N. 124TH STREET, SUITE J	BROOKFIELD	WI	53005
DOCUGRAPHICS, LLC	THOMAS	FIMIAN	2408A ASHLEY RIVER ROAD, SUITE 6-B	CHARLESTON	SC	29407
POTOMAC BUSINESS SOLUTIONS LLC	KRISTIN	JAQUETTE	13800 COPPERMINE ROAD, STE 273	HERNDON	VA	20171
DIGITAL OFFICE SOLUTIONS II	ROBERT	WEBB	4125 N. 124TH STREET, SUITE J	BROOKFIELD	WI	53005
RBI	RICK	BOWLING	1113B N. CASTLE HEIGHTS AVE	LEBANON	TN	37087
XCEL OFFICE SOLUTIONS	MICHAEL	REID	304 N MERIDIAN AVE STE 18	OKLAHOMA CITY	OK	73107
QUALITY PRINT SOLUTIONS	GENE	AYALA	220 N. GETTY STREET	UVALDE	TX	78801
IMAGE XCELLENCE, LLC	JENNIFER	CAMBIO	2123 KING STREET	LA CROSSE	WI	54601
CENTRAL OREGON OFFICE SOLUTIONS	RHONDA	ROGERS	PO BOX 2185	BEND	OR	97709
MAINE DOCUMENT SOLUTIONS, LLC	GABE	POLCHIES	59 SANFORD DRIVE, UNIT 1	GORHAM	ME	04038
OFFICE EQUIPMENT SOURCE, INC. (IV)	MIKE	MITCHELL	227 W. WATER STREET	ELMIRA	NY	14901
GULF SUPERIOR OFFICE PRODUCTS, INC. – SUPERIOR VI	RANDY	POCHE	533 HIGHLANDIA DRIVE, STE K	BATON ROUGE	LA	70810
ADVANCED DOCUMENT SOLUTIONS, INC. (IV)	SCOTT	HAMILTON	819 S. FLOYD STREET	LOUISVILLE	KY	40203
DOCUMENT TECHNOLOGIES, INC.	JANICE	DUPLISEA	23 CROSBY DRIVE	BEDFORD	MA	01730
METRO CENTRE, LP	KARLA	METZLER	679 COUNTY ROAD 404	GAINESVILLE	TX	76240
BENCHMARK BUSINESS SOLUTIONS, INC. (AMARILLO II)	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
DIGITAL OFFICE CENTRE, INC. (II)	TOM	ROSTVEDT	515 20TH AVENUE SE, STE 11	MINOT	ND	58701
XMC OF WEST TENNESSEE, INC.	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
NORTH COUNTRY DIGITAL SOLUTIONS	DAN	MCALOON	2 CRESTWOOD DRIVE	ALEXANDRIA BAY	NY	13607
SOLUTIONS FOR DOCUMENTS	MARVIN	HAMONS	3310 WOODVILLE RD, STE. C	NORTHWOOD	OH	43619
EAST-PENN BUSINESS MACHINES, INC.	HEMAN	PATEL	2980 LINDEN STREET	BETHLEHEM	PA	18017
YAKIMA DOCUMENT SOLUTIONS	LEE	HARTUNG	6799 N WENAS RD	SELAH	WA	98942
DOCUGRAPHICS, LLC	THOMAS	FIMIAN	2015 BOUNDARY ST, STE 232	BEAUFORT	SC	29902
MORRIS BUSINESS SOLUTIONS, LLC	RICHARD	MORRIS	P.O. BOX 15090	GREENVILLE	SC	29610
XMC OF NORTH ALABAMA, INC.	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
DOCUMENT CONSULTING SERVICES II	TED	SWICK	880 APOLLO STREET, SUITE 353	EL SEGUNDO	CA	90245

DIGITAL OFFICE SOLUTIONS, INC.	VIC	KALIA	311 3RD AVE, SE	CEDAR RAPIDS	IA	52401
CAPE COD BUSINESS SOLUTIONS, INC.	KEVIN	DONAHUE	PO BOX 323	SANDWICH	MA	02563
MARITIME BUSINESS CONCEPTS, INC. (II)	SCOTT	WILLIAMS	1306 N. HERRITAGE ST	KINSTON	NC	28501
SUPERIOR OFFICE PRODUCTS II	RANDY	POCHE	533 HIGHLANDIA DRIVE, STE K	BATON ROUGE	LA	70810
MAINE DOCUMENT SOLUTIONS OF CENTRAL MAINE	GABE	POLCHIES	59 SANFORD DRIVE, UNIT 1	GORHAM	ME	04038
TALLAHASSEE TECHNOLOGY GROUP, INC. (COLUMBUS)	RICHARD	MAUS	1949 RAYMOND DIEHL ROAD STE B	TALLAHASSEE	FL	32308
BUSINESS IMPRESSIONS OF MICHIGAN	JEFF	BASSETT	PO BOX 959	AUBURN	IN	46706
DOCUGRAPHICS, LLC	THOMAS	FIMIAN	2408 ASHLEY RIVER RD, UNIT A	CHARLESTON	SC	29414
DIGITAL OFFICE SOLUTIONS IV	ROBERT	WEBB	4125 N. 124TH STREET, SUITE J	BROOKFIELD	WI	53005
ASTRATECH, INC.	CHARLLEE	HOLMES	81 EAST GROVE STREET	GALESBURG	IL	61401
BENCHMARK BUSINESS SOLUTIONS, INC. (MARBLE FALLS)	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
BENCHMARK BUSINESS SOLUTIONS-WICHITA FALLS	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
JUSTTECH, LLC	JOSHUA	JUSTICE	101 CATALPA DR STE #102	LA PLATA	MD	20646
COMPLETE OFFICE SOLUTIONS	JOHN	COOPER	2627 RIDGEWOOD ROAD	JACKSON	MS	39216
ADVANCED DOCUMENT SOLUTIONS, INC.	SCOTT	HAMILTON	819 S. FLOYD STREET	LOUISVILLE	KY	40203
XMC OF MIDDLE TENNESSEE	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
XMC OF FLORENCE	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
COMPLETE DOCUMENT SOLUTIONS - MD LLC	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
SOUTHWEST OFFICE SOLUTIONS, INC. (TAOS)	TRACY	ASHTON	1789 CENTRAL AVENUE, SUITE 4	LOS ALAMOS	NM	87544
ELITE BUSINESS SYSTEMS, LLC	WILLIAM	ARNETT	P.O. BOX 737	GADSDEN	AL	35901
IMAGE MAKERS INC II	LAURA	NYQUIST	3588 VETERANS DRIVE, SUITE 3	TRAVERSE CITY	MI	49684
DOCUGRAPHICS, LLC	THOMAS	FIMIAN	454 ANDERSON RD. S, STE 152 BTC 571	ROCK HILL	SC	29730
MORRIS BUSINESS SOLUTIONS LLC (IV)	RICHARD	MORRIS	P.O. BOX 15090	GREENVILLE	SC	29610
SUPERIOR OFFICE PRODUCTS III	RANDY	POCHE	533 HIGHLANDIA DRIVE, STE K	BATON ROUGE	LA	70810
BENCHMARK BUSINESS SOLUTIONS-EL PASO	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
OFFICE EXPERTS, INC	KATHLEEN	SALIMBENE	520 HIGHRIDGE ROAD	LEXINGTON	OH	44904
PREFERRED DOCUMENT SOLUTIONS, LLC	CHRISTOPHER	SPAHN	2395 BRIARGATE BLVD, STE 120	COLORADO SPRINGS	CO	80920
ADVANTAGE BUSINESS SYSTEMS, INC.	MEIR	HOLTZBERG	370 STATE ST., SUITE 2	NORTH HAVEN	CT	06473
MIDWEST DATA SYSTEMS, INC.	KRISTIN	PORTER	10124 HUTTON ROAD	KANSAS CITY	KS	66109
DOCUGRAPHICS, LLC	THOMAS	FIMIAN	1201 MAIN STREET SUITE 1100	COLUMBIA	SC	29201
COPY SOLUTIONS, INC. (WEST)	ROGER	ZHAO	919 S. FREMONT AVE, SUITE 398	ALHAMBRA	CA	91803
BUTLER'S OFFICE EQUIPMENT & SUPPLY (WEST)	PATRICK	BUTLER	1900 E. HISTORIC HWY 66, SUITE C	GALLUP	NM	87301
REPRO PRODUCTS MFD, LLC (NORTH)	ROBERT	FELDBERG	4485 S ATLANTA RD	SMYRNA	GA	30080
REPRO PRODUCTS MFD, LLC (EAST)	ROBERT	FELDBERG	4485 S ATLANTA RD	SMYRNA	GA	30080
REPRO PRODUCTS MFD, LLC (SOUTH)	ROBERT	FELDBERG	4485 S ATLANTA RD	SMYRNA	GA	30080
BENCHMARK BUSINESS SOLUTIONS-SAN ANTONIO	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
SUPERIOR PRINT SOLUTIONS, INC.	BETHANY	SCHRIEVER	202 1st STREET SE, STE 103	MASON CITY	IA	50401
MORRIS BUSINESS SOLUTIONS, LLC (II)	RICHARD	MORRIS	P.O. BOX 15090	GREENVILLE	SC	29610
DOCUGRAPHICS, LLC	THOMAS	FIMIAN	2408 ASHLEY RIVER ROAD, SUITE 6-B	CHARLESTON	SC	29407

JUSTTECH, LLC (II)	JOSHUA	JUSTICE	101 CATALPA DR STE #102	LA PLATA	MD	20646
HAMILTON DIGITAL, INC. (CINCINNATI)	FRED	HAMILTON	2165 CENTRAL PARKWAY	CINCINNATI	OH	45219
GEYER'S OFFICE SUPPLY (II)	RON	GEYER	169 W. MAIN STREET	XENIA	OH	45385
IMAGE SOURCE - ORANGE COUNTY	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 540	SAN BERNARDINO	CA	92408
ITECH	MICHAEL	WILLIAMS	326 5TH STREET	PARKERSBURG	WV	26101
OFFICE EQUIPMENT SOURCE, INC. (III)	MIKE	MITCHELL	227 W. WATER STREET	ELMIRA	NY	14901
QUALITY QUICKLY (II)	BRIAN	MARSHALL	945 3rd AVE SE SUITE 103	HICKORY	NC	28602
RAY BLOCK STATIONERY II	GEORGE	GARCIA	3 PLAINFIELD AVE.	FLORAL PARK	NY	11001
MCGARITY'S BUSINESS PRODUCTS	SCOTT	MCGARITY	870 GROVE STREET	GAINSVILLE	GA	30501
IMAGE SOURCE - ORANGE COUNTY II	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 540	SAN BERNARDINO	CA	92408
DOCUMENT SOLUTIONS (III)	LOREN	MAUK	1540 RICE ROAD, SUITE 100	TYLER	TX	75703
XMC OF EAST TENNESSEE, INC.	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
SOUTHWEST OFFICE SOLUTIONS, INC. (SANTE FE)	TRACY	ASHTON	1789 CENTRAL AVENUE, SUITE 4	LOS ALAMOS	NM	87544
THE RAY-BLOCK STATIONERY CO. INC. (EAST)	GEORGE	GARCIA	3 PLAINFIELD AVE.	FLORAL PARK	NY	11001
COMPLETE DOCUMENT SOLUTIONS PA, LLC (S JERSEY I)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
COMPLETE DOCUMENT SOLUTIONS PA, LLC (S JERSEY II)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
COMPLETE DOCUMENT SOLUTIONS PA, LLC (PHL)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
COMPLETE DOCUMENT SOLUTIONS PA, LLC (PHL II)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
COMPLETE DOCUMENT SOLUTIONS, LLC (II)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
ALASKA ENTERPRISE SOLUTIONS, INC.	MICHAEL	FERRIS	557 E FIREWEED LN, SUITE A	ANCHORAGE	AK	99503
DOCUMENT SOLUTIONS (IV)	LOREN	MAUK	1540 RICE ROAD, SUITE 100	TYLER	TX	75703
BENCHMARK BUSINESS SOLUTIONS, INC. (AUSTIN)	JEFF	HORN	1607 BROADWAY	LUBBOCK	TX	79401
DMC2, INC.	KEVIN	FITZPATRICK	42 WORTHINGTON ACCESS DR	MARYLAND HEIGHTS	MO	63043
DMC2, INC. (II)	KEVIN	FITZPATRICK	42 WORTHINGTON ACCESS DR	MARYLAND HEIGHTS	MO	63043
SUPERIOR OFFICE PRODUCTS - BEAUMONT	RANDY	POCHE	533 HIGHLANDIA DRIVE, STE K	BATON ROUGE	LA	70810
D-TECH BUSINESS SOLUTIONS, LLC	FRANK	DEFRANCESCO	1095 MILITARY TRL, UNIT 1447	JUPITER	FL	33458
DIGITAL DOCUMENT SOLUTIONS, LLC	BRIDGET	EVANS	901 LAKE ROAD	MOUNTAIN TOP	PA	18707
IMAGE SOURCE (SAN DIEGO)	BRAD	CRAFT	650 EAST HOSPITALITY LANE, STE 540	SAN BERNARDINO	CA	92408
NAPLES OFFICE SOLUTIONS, LLC	CHRIS	DEICHMAN	3449 TECHNOLOGY DRIVE STE 108	NORTH VENICE	FL	34275
ADVANCED OFFICE SOLUTIONS, LLC	JOHN	BARROW	4124 KESTEVEN DRIVE	BIRMINGHAM	AL	35242
AMERICAN BUSINESS CENTER, INC.	RICHARD	YEATS	PO BOX 20128	PANAMA CITY	FL	32417
OFFICE EQUIPMENT SOURCE, INC. (V)	MIKE	MITCHELL	227 W. WATER STREET	ELMIRA	NY	14901
BENCHMARK OFFICE SYSTEMS INC. (WEST)	MICHELLE	MCMANUS	75 GILCREAST RD., STE. 311	LONDONDERRY	NH	03053
COMPLETE DOCUMENT SOLUTIONS, WC-CT, LLC (I)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
COMPLETE DOCUMENT SOLUTIONS, MARYLAND LLC (II)	JOHN	HAND	19 GLORIA LANE	FAIRFIELD	NJ	07004
COASTAL OREGON OFFICE SOLUTIONS	RHONDA	ROGERS	PO BOX 2185	BEND	OR	97709
SOUTHWEST OFFICE SOLUTIONS, INC. (ALBUQUERQUE)	TRACY	ASHTON	1789 CENTRAL AVENUE, SUITE 4	LOS ALAMOS	NM	87544
XMC, INC. (SOUTH ARKANSAS)	BOB	HAMILTON	7585 AE BEATY DRIVE, SUITE 101	BARTLETT	TN	38133
MORRIS BUSINESS SOLUTIONS, LLC (III)	RICHARD	MORRIS	P.O. BOX 15090	GREENVILLE	SC	29610

Xerox US Enterprise Operations
Xerox Government, Healthcare and Education

Region	VP Sales	Email
Southeast	Steve Pitts	Steve.Pitts@Xerox.com
Mid America	Jorge Galindez	Jorge.Galindez@Xerox.com
Northeast	Chris Goodwin	Chris.Goodwin@Xerox.com
Texas/Oklahoma	Kelly Grotheer	Kelly.Grotheere@Xerox.com
West	Michelle Yoshino	Michelle.Yoshino@Xerox.com

**OMNIA PARTNERS EXHIBITS
EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS**

**FEDERAL CERTIFICATIONS
ADDENDUM FOR AGREEMENT FUNDED BY U.S. FEDERAL GRANT**

TO WHOM IT MAY CONCERN:

Participating Agencies may elect to use federal funds to purchase under the Master Agreement. This form should be completed and returned.

DEFINITIONS

Contract means a legal instrument by which a non-Federal entity purchases property or services needed to carry out the project or program under a Federal award. The term as used in this part does not include a legal instrument, even if the non-Federal entity considers it a contract, when the substance of the transaction meets the definition of a Federal award or subaward

Contractor means an entity that receives a contract as defined in Contract.

Cooperative agreement means a legal instrument of financial assistance between a Federal awarding agency or pass-through entity and a non-Federal entity that, consistent with 31 U.S.C. 6302-6305:

(a) Is used to enter into a relationship the principal purpose of which is to transfer anything of value from the Federal awarding agency or pass-through entity to the non-Federal entity to carry out a public purpose authorized by a law of the United States (see 31 U.S.C. 6101(3)); and not to acquire property or services for the Federal government or pass-through entity's direct benefit or use;

(b) Is distinguished from a grant in that it provides for substantial involvement between the Federal awarding agency or pass-through entity and the non-Federal entity in carrying out the activity contemplated by the Federal award.

(c) The term does not include:

(1) A cooperative research and development agreement as defined in 15 U.S.C. 3710a; or

(2) An agreement that provides only:

(i) Direct United States Government cash assistance to an individual;

(ii) A subsidy;

(iii) A loan;

(iv) A loan guarantee; or

(v) Insurance.

Federal awarding agency means the Federal agency that provides a Federal award directly to a non-Federal entity

Federal award has the meaning, depending on the context, in either paragraph (a) or (b) of this section:

(a)(1) The Federal financial assistance that a non-Federal entity receives directly from a Federal awarding agency or indirectly from a pass-through entity, as described in § 200.101 Applicability; or

(2) The cost-reimbursement contract under the Federal Acquisition Regulations that a non-Federal entity receives directly from a Federal awarding agency or indirectly from a pass-through entity, as described in § 200.101 Applicability.

(b) The instrument setting forth the terms and conditions. The instrument is the grant agreement, cooperative agreement, other agreement for assistance covered in paragraph (b) of § 200.40 Federal financial assistance, or the cost-reimbursement contract awarded under the Federal Acquisition Regulations.

(c) Federal award does not include other contracts that a Federal agency uses to buy goods or services from a contractor or a contract to operate Federal government owned, contractor operated facilities (GOCOs).

(d) See also definitions of Federal financial assistance, grant agreement, and cooperative agreement.

Non-Federal entity means a state, local government, Indian tribe, institution of higher education (IHE), or nonprofit organization that carries out a Federal award as a recipient or subrecipient.

Nonprofit organization means any corporation, trust, association, cooperative, or other organization, not including IHEs, that:

(a) Is operated primarily for scientific, educational, service, charitable, or similar purposes in the public interest;

(b) Is not organized primarily for profit; and

OMNIA PARTNERS EXHIBITS

EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

Pursuant to Federal Rule (F) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (F) above.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

(G) Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended—Contracts and subgrants of amounts in excess of \$150,000 must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401-7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251- 1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA)

Pursuant to Federal Rule (G) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency member resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (G) above.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

(H) Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the Executive Office of the President Office of Management and Budget (OMB) guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Pursuant to Federal Rule (H) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency. If at any time during the term of an award the offeror or its principals becomes debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency, the offeror will notify the Participating Agency.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

(I) Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)—Contractors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

Pursuant to Federal Rule (I) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term and after the awarded term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). The undersigned further certifies that:

(1) No Federal appropriated funds have been paid or will be paid for on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall

OMNIA PARTNERS EXHIBITS

EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying", in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all covered sub-awards exceeding \$100,000 in Federal funds at all appropriate tiers and that all subrecipients shall certify and disclose accordingly.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

RECORD RETENTION REQUIREMENTS FOR CONTRACTS INVOLVING FEDERAL FUNDS

When federal funds are expended by Participating Agency for any contract resulting from this procurement process, offeror certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.333. The offeror further certifies that offeror will retain all records as required by 2 CFR § 200.333 for a period of three years after grantees or subgrantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF COMPLIANCE WITH THE ENERGY POLICY AND CONSERVATION ACT

When Participating Agency expends federal funds for any contract resulting from this procurement process, offeror certifies that it will comply with the mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6321 et seq.; 49 C.F.R. Part 18).

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF COMPLIANCE WITH BUY AMERICA PROVISIONS

To the extent purchases are made with Federal Highway Administration, Federal Railroad Administration, or Federal Transit Administration funds, offeror certifies that its products comply with all applicable provisions of the Buy America Act and agrees to provide such certification or applicable waiver with respect to specific products to any Participating Agency upon request. Purchases made in accordance with the Buy America Act must still follow the applicable procurement rules calling for free and open competition.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF ACCESS TO RECORDS - 2 C.F.R. § 200.336

Offeror agrees that the Inspector General of the Agency or any of their duly authorized representatives shall have access to any documents, papers, or other records of offeror that are pertinent to offeror's discharge of its obligations under the Contract for the purpose of making audits, examinations, excerpts, and transcriptions. The right also includes timely and reasonable access to offeror's personnel for the purpose of interview and discussion relating to such documents.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

CERTIFICATION OF APPLICABILITY TO SUBCONTRACTORS

Offeror agrees that all contracts it awards pursuant to the Contract shall be bound by the foregoing terms and conditions.

Does offeror agree? YES [Signature] Initials of Authorized Representative of offeror

Offeror agrees to comply with all federal, state, and local laws, rules, regulations and ordinances, as applicable. It is further acknowledged that offeror certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted above.

Offeror's Name: Xerox Corporation

Address, City, State, and Zip Code: 201 Merritt 7, Norwalk, CT 06857

OMNIA PARTNERS EXHIBITS
EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

Phone Number: 310-258-6266 Fax Number: _____

Printed Name and Title of Authorized Representative: Rachael Jones Turner, SLED Cooperative Contracts Manager

Email Address: Rachael.Jones@Xerox.com

Signature of Authorized Representative: Rachael Jones Turner Date: 6/2/2020

XEROX CORPORATION

Certificate of Secretary

I, Douglas H. Marshall, Secretary of Xerox Corporation, a New York corporation (the "Company"), DO HEREBY CERTIFY that:

1. The following is a true and correct copy of an excerpt from a resolution duly adopted at a meeting of the Board of Directors of the Company duly held and convened on December 7, 2011, at which meeting a duly constituted quorum of the Board of Directors was present and acting throughout and that such resolution has not been modified, rescinded or revoked and is at present in full force and effect:

RESOLVED: that ... the President, any Vice President, the Treasurer, the Controller and any Manager or Director of any group, division or department of the Company, be, and each of them severally is, empowered to (i) execute and deliver in the name and on behalf of the Company all agreements, contracts, bids, instruments of conveyance or encumbrance, leases, bonds, consents, certificates (including any non-collusion certificates required by any governmental entity, department, agency or official), releases, powers of attorney and other documents which may be necessary or desirable in and relating to the ordinary conduct of the business of the group, division or department which he serves in that capacity (all of the foregoing collectively referred to as "Agreements") (ii) perform under agreements or cause to be performed, the Company's obligations under all such Agreements; and (iii) from time to time delegate their authority under this resolution to such employees of the Company and subject to such terms, conditions and limitations as they determine to be advisable, the execution and delivery of any such delegation to be conclusive evidence of such determination.

2. Joanne Levy is as of the date hereof Account General Manager, New York City, New Jersey and Pennsylvania, in the Public Sector Center of Excellence, North America Operations, of the Company and is authorized to act under the above resolution.

IN WITNESS WHEREOF, the undersigned has executed this Certificate and affixed the corporate seal of the Company hereto as of the 20th day of May, 2019.



Douglas H. Marshall
Secretary



OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE

NEW JERSEY BUSINESS COMPLIANCE

Suppliers intending to do business in the State of New Jersey must comply with policies and procedures required under New Jersey statutes. All offerors submitting proposals must complete the following forms specific to the State of New Jersey. Completed forms should be submitted with the offeror's response to the RFP. Failure to complete the New Jersey packet will impact OMNIA Partners's ability to promote the Master Agreement in the State of New Jersey.

- DOC #1 Ownership Disclosure Form
- DOC #2 Non-Collusion Affidavit
- DOC #3 Affirmative Action Affidavit
- DOC #4 Political Contribution Disclosure Form
- DOC #5 Stockholder Disclosure Certification
- DOC #6 Certification of Non-Involvement in Prohibited Activities in Iran
- DOC #7 New Jersey Business Registration Certificate

New Jersey suppliers are required to comply with the following New Jersey statutes when applicable:

- all anti-discrimination laws, including those contained in N.J.S.A. 10:2-1 through N.J.S.A. 10:2-14, N.J.S.A. 10:5-1, and N.J.S.A. 10:5-31 through 10:5-38;
- Prevailing Wage Act, N.J.S.A. 34:11-56.26, for all contracts within the contemplation of the Act;
- Public Works Contractor Registration Act, N.J.S.A. 34:11-56.26; and
- Bid and Performance Security, as required by the applicable municipal or state statutes.

**OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE**

DOC #1

**OWNERSHIP DISCLOSURE FORM
(N.J.S. 52:25-24.2)**

Pursuant to the requirements of P.L. 1999, Chapter 440 effective April 17, 2000 (Local Public Contracts Law), the offeror shall complete the form attached to these specifications listing the persons owning 10 percent (10%) or more of the firm presenting the proposal.

Company Name: Xerox Corporation
Street: 201 Merritt 7
City, State, Zip Code: Norwalk, CT 06851

Complete as appropriate:

I _____, certify that I am the sole owner of _____, that there are no partners and the business is not incorporated, and the provisions of N.J.S. 52:25-24.2 do not apply.

OR:

I _____, a partner in _____, do hereby certify that the following is a list of all individual partners who own a 10% or greater interest therein. I further certify that if one (1) or more of the partners is itself a corporation or partnership, there is also set forth the names and addresses of the stockholders holding 10% or more of that corporation's stock or the individual partners owning 10% or greater interest in that partnership.

OR:

I, Douglas H. Marshall, an authorized representative of Xerox Corporation, a corporation, do hereby certify that the following is a list of the names and addresses of all stockholders in the corporation who own 10% or more of its stock of any class. I further certify that if one (1) or more of such stockholders is itself a corporation or partnership, that there is also set forth the names and addresses of the stockholders holding 10% or more of the corporation's stock or the individual partners owning a 10% or greater interest in that partnership. (Note: information is as of December 31, 2019)

(Note: If there are no partners or stockholders owning 10% or more interest, indicate none.)

Name	Address	Interest
Carl C. Icahn	c/o Icahn Capital LP 767 Fifth Avenue, Suite 4700 New York, NY 10153	10.99%
The Vanguard Group, Inc.	100 Vanguard Blvd. Malvern, PA 19355	10.32%

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

May 8, 2020
Date



Secretary

Authorized Signature and Title

Requirements for National Cooperative Contract

OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE

DOC #2

NON-COLLUSION AFFIDAVIT

Company Name: Xerox Corporation
Street: 201 Merritt 7
City, State, Zip Code: Norwalk, CT 06851

State of New Jersey
County of Middlesex

I, Joanne Levy of the Woodbridge
Name City

in the County of Middlesex, State of New Jersey
of full age, being duly sworn according to law on my oath depose and say that:

I am the General Manager of the firm of Xerox Corporation
Title Company Name

the Offeror making the Proposal for the goods, services or public work specified under the attached proposal, and that I executed the said proposal with full authority to do so; that said Offeror has not directly or indirectly entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free, competitive bidding in connection with the above proposal, and that all statements contained in said proposal and in this affidavit are true and correct, and made with full knowledge that relies upon the truth of the statements contained in said proposal and in the statements contained in this affidavit in awarding the contract for the said goods, services or public work.

I further warrant that no person or selling agency has been employed or retained to solicit or secure such contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee, except bona fide employees or bona fide established commercial or selling agencies maintained by

Xerox Corporation
Company Name

[Signature] GM State of NJ
Authorized Signature & Title

Subscribed and sworn before me

this 16th day of May, 2020

Terrence Horsley
Notary Public of New Jersey

My commission expires September 2, 2024

TERRENCE HORSLEY
NOTARY PUBLIC
STATE OF NEW JERSEY
ID # 2229180
MY COMMISSION EXPIRES SEPTEMBER 2, 2024



OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE

DOC #3

AFFIRMATIVE ACTION AFFIDAVIT
(P.L. 1975, C.127)

Company Name: Xerox Corporation
Street: 201 Merritt 7
City, State, Zip Code: Norwalk, CT 06851

Proposal Certification:

Indicate below company's compliance with New Jersey Affirmative Action regulations. Company's proposal will be accepted even if company is not in compliance at this time. No contract and/or purchase order may be issued, however, until all Affirmative Action requirements are met.

Required Affirmative Action Evidence:

Procurement, Professional & Service Contracts (Exhibit A)

Vendors must submit with proposal:

- 1. A photo copy of their Federal Letter of Affirmative Action Plan Approval

OR

- 2. A photo copy of their Certificate of Employee Information Report

OR

- 3. A complete Affirmative Action Employee Information Report (AA302)

Public Work – Over \$50,000 Total Project Cost:

- A. No approved Federal or New Jersey Affirmative Action Plan. We will complete Report Form AA201-A upon receipt from the
- B. Approved Federal or New Jersey Plan – certificate enclosed

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

5/11/2020
Date

[Signature]
Authorized Signature and Title

**OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE**

DOC #3, continued

**P.L. 1995, c. 127 (N.J.A.C. 17:27)
MANDATORY AFFIRMATIVE ACTION LANGUAGE**

**PROCUREMENT, PROFESSIONAL AND SERVICE
CONTRACTS**

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. The contractor will take affirmative action to ensure that such applicants are recruited and employed, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this non-discrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisement for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation.

The contractor or subcontractor, where applicable, will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice, to be provided by the agency contracting officer advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to P.L. 1975, c. 127, as amended and supplemented from time to time and the Americans with Disabilities Act.

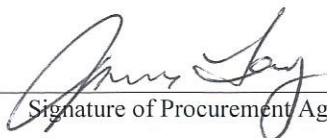
The contractor or subcontractor agrees to attempt in good faith to employ minority and female workers trade consistent with the applicable county employment goal prescribed by N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time or in accordance with a binding determination of the applicable county employment goals determined by the Affirmative Action Office pursuant to N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time.

The contractor or subcontractor agrees to inform in writing appropriate recruitment agencies in the area, including employment agencies, placement bureaus, colleges, universities, labor unions, that it does not discriminate on the basis of age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of it testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the state of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

The contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and lay-off to ensure that all such actions are taken without regard to age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and conform with the applicable employment goals, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor and its subcontractors shall furnish such reports or other documents to the Affirmative Action Office as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Affirmative Action Office for conducting a compliance investigation pursuant to Subchapter 10 of the Administrative Code (NJAC 17:27).



Signature of Procurement Agent

Requirements for National Cooperative Contract

Certification 1160

**CERTIFICATE OF EMPLOYEE INFORMATION REPORT
RENEWAL**

This is to certify that the contractor listed below has submitted an Employee Information Report pursuant to N.J.A.C. 17:27-1.1 et. seq. and the State Treasurer has approved said report. This approval will remain in effect for the period of **15-MAR-2019** to **15-MAR-2022**



**XEROX CORPORATION
10 WOODBRIDGE CENTER DR.
WOODBRIDGE NJ 07095**

Elizabeth M. Muoio

ELIZABETH MAHER MUOIO
State Treasurer

OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE

DOC #4

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM
Public Agency Instructions

This page provides guidance to public agencies entering into contracts with business entities that are required to file Political Contribution Disclosure forms with the agency. **It is not intended to be provided to contractors.** What follows are instructions on the use of form local units can provide to contractors that are required to disclose political contributions pursuant to N.J.S.A. 19:44A-20.26 (P.L. 2005, c. 271, s.2). Additional information on the process is available in Local Finance Notice 2006-1 (http://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html). Please refer back to these instructions for the appropriate links, as the Local Finance Notices include links that are no longer operational.

1. The disclosure is required for all contracts in excess of \$17,500 that are **not awarded** pursuant to a “fair and open” process (N.J.S.A. 19:44A-20.7).
2. Due to the potential length of some contractor submissions, the public agency should consider allowing data to be submitted in electronic form (i.e., spreadsheet, pdf file, etc.). Submissions must be kept with the contract documents or in an appropriate computer file and be available for public access. **The form is worded to accept this alternate submission.** The text should be amended if electronic submission will not be allowed.
3. The submission must be **received from the contractor and** on file at least 10 days prior to award of the contract. Resolutions of award should reflect that the disclosure has been received and is on file.
4. The contractor must disclose contributions made to candidate and party committees covering a wide range of public agencies, including all public agencies that have elected officials in the county of the public agency, state legislative positions, and various state entities. The Division of Local Government Services recommends that contractors be provided a list of the affected agencies. This will assist contractors in determining the campaign and political committees of the officials and candidates affected by the disclosure.
 - a. The Division has prepared model disclosure forms for each county. They can be downloaded from the “County PCD Forms” link on the Pay-to-Play web site at <http://www.nj.gov/dca/divisions/dlgs/programs/lpcl.html#12>. They will be updated from time-to-time as necessary.
 - b. A public agency using these forms **should edit them to properly reflect the correct legislative district(s)**. As the forms are county-based, **they list all legislative districts** in each county. **Districts that do not represent the public agency should be removed from the lists.**
 - c. Some contractors may find it easier to provide a single list that covers all contributions, regardless of the county. These submissions are appropriate and should be accepted.
 - d. The form may be used “as-is”, subject to edits as described herein.
 - e. The “Contractor Instructions” sheet is intended to be provided with the form. It is recommended that the Instructions and the form be printed on the same piece of paper. The form notes that the Instructions are printed on the back of the form; where that is not the case, the text should be edited accordingly.
 - f. The form is a Word document and can be edited to meet local needs, and posted for download on web sites, used as an e-mail attachment, or provided as a printed document.
5. It is recommended that the contractor also complete a “Stockholder Disclosure Certification.” This will assist the local unit in its obligation to ensure that contractor did not make any prohibited contributions to the committees listed on the Business Entity Disclosure Certification in the 12 months prior to the contract (See Local Finance Notice 2006-7 for additional information on this obligation at http://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html). A sample Certification form is part of this package and the instruction to complete it is included in the Contractor Instructions. NOTE: This section is not applicable to Boards of Education.

OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE

Doc #4, continued **C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM**

Contractor Instructions

Business entities (contractors) receiving contracts from a public agency that are NOT awarded pursuant to a "fair and open" process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s.2 (N.J.S.A. 19:44A-20.26). This law provides that 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

- any State, county, or municipal committee of a political party
- any legislative leadership committee*
- any continuing political committee (a.k.a., political action committee)
- any candidate committee of a candidate for, or holder of, an elective office:
 - of the public entity awarding the contract
 - of that county in which that public entity is located
 - of another public entity within that county
 - or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county

The disclosure must list reportable contributions to any of the committees that exceed \$300 per election cycle that were made during the 12 months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- individuals with an "interest" ownership or control of more than 10% of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit
- all principals, partners, officers, or directors of the business entity or their spouses
- any subsidiaries directly or indirectly controlled by the business entity
- IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity and filing as continuing political committees, (PACs).

When the business entity is a natural person, "a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity." [N.J.S.A. 19:44A-20.26(b)] The contributor must be listed on the disclosure.

Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report.

The enclosed list of agencies is provided to assist the contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor's responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement.

The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed cover sheet) may be used as the contractor's submission and is disclosable to the public under the Open Public Records Act.

The contractor must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law. **NOTE: This section does not apply to Board of Education contracts.**

* N.J.S.A. 19:44A-3(s): "The term "legislative leadership committee" means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L.1993, c.65 (C.19:44A-10.1) for the purpose of receiving contributions and making expenditures."

Requirements for National Cooperative Contract

**OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE**

**List of Agencies with Elected Officials Required for Political Contribution Disclosure
N.J.S.A. 19:44A-20.26**

County Name:

State: Governor, and Legislative Leadership Committees

Legislative District #s:

State Senator and two members of the General Assembly per district.

County:

Freeholders

County Clerk

Sheriff

{County Executive}

Surrogate

Municipalities (Mayor and members of governing body, regardless of title):

**USERS SHOULD CREATE THEIR OWN FORM, OR DOWNLOAD
FROM THE PAY TO PLAY SECTION OF THE DLGS WEBSITE A
COUNTY-BASED, CUSTOMIZABLE FORM.**

OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE

DOC #5

STOCKHOLDER DISCLOSURE CERTIFICATION

Name of Business:

I certify that the list below contains the names and home addresses of all stockholders holding 10% or more of the issued and outstanding stock of the undersigned.

OR

I certify that no one stockholder owns 10% or more of the issued and outstanding stock of the undersigned.

Check the box that represents the type of business organization:

Partnership

Corporation

Sole Proprietorship

Limited Partnership

Limited Liability Corporation

Limited Liability Partnership

Subchapter S Corporation

Sign and notarize the form below, and, if necessary, complete the stockholder list below.

Stockholders:

Name: Carl C Icahn	Name: The Vanguard Group
Home Address: Business Address: C/o Icahn Capital LP 767 5th Ave NY 10153	Home Address: 100 Vanguard Bvd. Business Address Malvern, Pa 19355
Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:

Subscribed and sworn before me this 11th day of May, 2020

(Notary Public) [Signature]

My Commission expires: 9/2/2024

[Signature]
(Affiant)

Jeanne Levy Cm. Secretary
(Print name & title of affiant)

(Corporate Seal)

TERRENCE HORSLEY
NOTARY PUBLIC
STATE OF NEW JERSEY
ID # 2229180
MY COMMISSION EXPIRES SEPTEMBER 2, 2024

Requirements for National Cooperative Contract

OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE

DOC #6

Certification of Non-Involvement in Prohibited Activities in Iran

Pursuant to N.J.S.A. 52:32-58, Offerors must certify that neither the Offeror, nor any of its parents, subsidiaries, and/or affiliates (as defined in N.J.S.A. 52:32 – 56(e) (3)), is listed on the Department of the Treasury's List of Persons or Entities Engaging in Prohibited Investment Activities in Iran and that neither is involved in any of the investment activities set forth in N.J.S.A. 52:32 – 56(f).

Offerors wishing to do business in New Jersey through this contract must fill out the Certification of Non-Involvement in Prohibited Activities in Iran here:

http://www.state.nj.us/humanservices/dfd/info/standard/fdc/disclosure_investmentact.pdf.

Offerors should submit the above form completed with their proposal.

STATE OF NEW JERSEY -- DIVISION OF PURCHASE AND PROPERTY
DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN

Quote Number: _____

Bidder/Offeree: Xerox Corporation

PART 1: CERTIFICATION

BIDDERS MUST COMPLETE PART 1 BY CHECKING EITHER BOX.

FAILURE TO CHECK ONE OF THE BOXES WILL RENDER THE PROPOSAL NON-RESPONSIVE.

Pursuant to Public Law 2012, c. 25, any person or entity that submits a bid or proposal or otherwise proposes to enter into or renew a contract must complete the certification below to attest, under penalty of perjury, that neither the person or entity, nor any of its parents, subsidiaries, or affiliates, is identified on the Department of Treasury's Chapter 25 list as a person or entity engaging in investment activities in Iran. The Chapter 25 list is found on the Division's website at <http://www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf>. Bidders must review this list prior to completing the below certification. **Failure to complete the certification will render a bidder's proposal non-responsive.** If the Director finds a person or entity to be in violation of law, s/he shall take action as may be appropriate and provided by law, rule or contract, including but not limited to, imposing sanctions, seeking compliance, recovering damages, declaring the party in default and seeking debarment or suspension of the party

PLEASE CHECK THE APPROPRIATE BOX:

I certify, pursuant to Public Law 2012, c. 25, that neither the bidder listed above nor any of the bidder's parents, subsidiaries, or affiliates is listed on the N.J. Department of the Treasury's list of entities determined to be engaged in prohibited activities in Iran pursuant to P.L. 2012, c. 25 ("Chapter 25 List"). I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf. **I will skip Part 2 and sign and complete the Certification below.**

OR

I am unable to certify as above because the bidder and/or one or more of its parents, subsidiaries, or affiliates is listed on the Department's Chapter 25 list. I will provide a detailed, accurate and precise description of the activities in Part 2 below and sign and complete the Certification below. Failure to provide such will result in the proposal being rendered as non-responsive and appropriate penalties, fines and/or sanctions will be assessed as provided by law.

PART 2: PLEASE PROVIDE FURTHER INFORMATION RELATED TO INVESTMENT ACTIVITIES IN IRAN

You must provide a detailed, accurate and precise description of the activities of the bidding person/entity, or one of its parents, subsidiaries or affiliates, engaging in the investment activities in Iran outlined above by completing the boxes below.

EACH BOX WILL PROMPT YOU TO PROVIDE INFORMATION RELATIVE TO THE ABOVE QUESTIONS. PLEASE PROVIDE THOROUGH ANSWERS TO EACH QUESTION. IF YOU NEED TO MAKE ADDITIONAL ENTRIES, CLICK THE "ADD AN ADDITIONAL ACTIVITIES ENTRY" BUTTON.

Name _____	Relationship to Bidder/Offeree _____
Description of Activities _____	
Duration of Engagement _____	Anticipated Cessation Date _____
Bidder/Offeree Contact Name _____	Contact Phone Number _____

ADD AN ADDITIONAL ACTIVITIES ENTRY

Certification: I, being duly sworn upon my oath, hereby represent and state that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I attest that I am authorized to execute this certification on behalf of the above-referenced person or entity. I acknowledge that the State of New Jersey is relying on the information contained herein and thereby acknowledge that I am under a continuing obligation from the date of this certification through the completion of any contracts with the State to notify the State in writing of any changes to the answers of information contained herein. I acknowledge that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I recognize that I am subject to criminal prosecution under the law and that it will also constitute a material breach of my agreement(s) with the State of New Jersey and that the State at its option may declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print): Joanne Levy

Signature: _____

Title: General Manager, State of New Jersey

Date: 5/11/2020

**OMNIA PARTNERS EXHIBITS
EXHIBIT G- NEW JERSEY BUSINESS COMPLIANCE**

DOC #7

**NEW JERSEY BUSINESS REGISTRATION CERTIFICATE
(N.J.S.A. 52:32-44)**

Offerors wishing to do business in New Jersey must submit their State Division of Revenue issued Business Registration Certificate with their proposal here. Failure to do so will disqualify the Offeror from offering products or services in New Jersey through any resulting contract.

<http://www.state.nj.us/treasury/revenue/forms/njreg.pdf>



STATE OF NEW JERSEY BUSINESS REGISTRATION CERTIFICATE

Taxpayer Name: XEROX CORPORATION

Trade Name:

Address: 201 MERRITT 7
NORWALK, CT 06851

Certificate Number: 0061020

Effective Date: November 07, 1960

Date of Issuance: July 16, 2018

For Office Use Only:

20180716081443468