

University of California (UC)

Contract # 2021003177

for

IT Security Tools

Data Detection (Category 2)

with

Spirion

Effective: November 4, 2021

The following documents comprise the executed contract between the University of California, Office of the President and Spirion effective November 4, 2021:

- I. Executed Purchasing Agreement
- II. Supplier's Response to the RFP, incorporated by reference.



UNIVERSITY OF CALIFORNIA

Purchasing Agreement #2021003177

The Agreement to furnish certain cloud computing services described herein and, in the documents, referenced herein (“Goods and/ or Services”), is made by and between The Regents of the University of California, a California public corporation (“UC”) on behalf of the University of California, and Spirion, a Delaware limited liability company with its principal place of business located at 200 Central Ave., Ste. 1900, St. Petersburg, FL, 33701. (“Supplier”). This Agreement is binding only if it is negotiated and executed by an authorized representative with the proper delegation of authority.

The terms and conditions of this Agreement will supersede and take precedence over those of any pre-existing agreement between any UC Location and Supplier as of the Effective Date of this Agreement. For purposes of this Agreement, a UC Location shall include but not be limited to all current and future UC Locations of the University of California and its Affiliates as further detailed at <https://www.universityofcalifornia.edu/uc-system/parts-of-uc>.

1. Statement of Work

Supplier agrees to provide the Goods and/or Services described in the statement of work attached as **Attachment “A”** (“UC Statement of Work”) and any other documents referenced in the Incorporated Documents section herein, at the prices set forth in the Statement of Work and any other documents referenced in the Incorporated Documents section herein. Unless otherwise provided in the Agreement, UC will not be obligated to purchase a minimum amount of Goods and/or Services from Supplier

2. Term of Agreement/Termination

- a. The Agreement is effective on the date of the final signature below (“Effective Date”). The initial term of the Agreement will be for 5 years after the Effective Date (Initial Term), and is subject to earlier termination as provided below.
- b. UC may renew the Agreement for 5 successive 1-year periods (each, a Renewal Term), by providing Supplier with at least 30 calendar days’ written notice before the end of the Initial Term or any Renewal Term.
- c. UC may terminate the Agreement for convenience by giving Supplier at least 30 calendar days’ written notice.
- d. UC or Supplier may terminate the Agreement for cause by giving the other party at least 30 days’ notice to cure a breach of the Agreement (Cure Period). If the breaching party fails to cure the breach within the Cure Period, the non-breaching party may immediately terminate the Agreement.

3. Scope of Agreement

- a) If Supplier eliminates any functionality of any of the Services provided under this Agreement and subsequently offers that functionality in other or new products (whether directly or indirectly through agreement with a third party), then the portion of those other or new products that contain the functionality in question, or the entire product if the functionality cannot be separated out, will be provided to UC at no additional charge and under the terms of this Agreement, including technical support. If Supplier incorporates the functionality of the Services provided under this Agreement into a newer product and continues to offer both products, UC may, in its sole discretion, exercise the option to upgrade to the newer product at no additional cost. Regardless of whether the functionality of the Services is impacted, Supplier will notify UC of any name changes in any Services within the earlier of thirty (30) calendar days of such change or thirty (30) days of when UC asks whether Supplier has made any name changes in the Services.
- b) UC and the users authorized by UC will have the right to access and use the Services at any location.

4. Rights and License In and To UC Data

- a) UC retains the right to use the Services to access and retrieve Institutional Information (as defined in the UC Appendix – Data Security and Privacy) stored on Supplier's Services infrastructure at any time at UC's sole discretion. If UC requests the Non-public Information from Supplier, Supplier will provide UC with copies within forty-eight (48) hours after receipt of a request from UC, and will cooperate with UC's reasonable requests in connection with its response.
- b) Supplier will return all Institutional Information to UC in a commonly used, non-proprietary, and mutually agreed upon format.

5. Service Levels

- a) Supplier represents and warrants that the Services will be performed in accordance with the attached document entitled *Spirion Customer Support Services and Service Level Agreement*, Attachment B to this Agreement
- b) If UC has concerns regarding Supplier's service levels, UC may escalate these concerns to its assigned Customer Success Manager (CSM):
 - c) Supplier will provide UC with a refund for all unachieved service levels no later than the thirtieth calendar (30th) calendar day of the month following the month in which the service levels was not achieved.
- d) Upon the request of the UC, Supplier will provide UC reports documenting its compliance with the service levels detailed herein. Reports will include, but not be limited to, providing the following information, to the degree that such information exists and can be transmitted to the UC in a readily human-readable form:
 - i) Monthly Services availability by percent time, dates and minutes that Services were not available, and identification of months in which agreed upon service levels were not achieved;
 - ii) Average transaction processing time per week, the fastest and slowest individual transaction processing time per week, the percent of transactions processed that meet the service levels stated herein, and identification of weeks in which agreed upon service levels are not met.
- e) UC retains the right to retain a third party to validate Supplier's performance in meeting agreed upon service levels.

6. Technical Support

- a) During the term of this Agreement Supplier will provide UC with ongoing technical support for the Services at no less than the levels and in the manner(s) specified herein.
- b) Supplier may not withdraw technical support for any Service without twelve (12) months advance written notice to UC, and then only if Supplier is withdrawing technical support from all of its customers.
- c) UC acquires the right to access and use technical support acquired under this Agreement at any location.
- d) UC will receive at its option the general help desk technical support offered by Supplier to its other customers. Irrespective of Supplier's general technical support offerings, Supplier will provide UC at UC's option with the following technical support:
 - i) Supplier will provide technical support to UC for the purpose of answering questions relating to the Services, including (a) clarification of functions and features of the Services; (b) clarification of the Documentation; (c) guidance in the operation of the Services; and (d) error verification, analysis, and correction, including the failure to produce results in accordance with the Documentation.
- e) Such assistance will be provided per Section B of the attached document entitled *Spirion Support Services and Service Level Agreement*.
- f) The following provisions will be applicable to the correction of Services errors:
 - i) If UC detects what it considers to be an error in the Services which causes it not to conform to, or produce results in accordance with, the Documentation, then UC will by telephone or e-mail notify Supplier of the error.
 - ii) Supplier will respond in accordance with Section A of the attached document entitled *Spirion Support Services and Service Level Agreement* for assistance in correcting or creating a workaround for a Services error. Supplier's response will include assigning fully-qualified technicians to work with UC to diagnose and correct or create a workaround for the Services error and notifying UC's representative making the initial request for assistance of Supplier's efforts, plans for resolution of the error, and estimated time required to resolve the error.
 - iii) Supplier will provide a correction or workaround acceptable to UC in accordance with Section A the attached document entitled *Spirion Support Services and Service Level Agreement*.
- g) The following provisions will set forth Supplier's obligations to provide Enhancements:
 - i) Supplier will generally enhance and improve the Services for as long as UC elects to receive and pays for the Services.
 - ii) Supplier will provide to UC during the Agreement term, (a) any and all Enhancements which it develops with respect to the Services; (b) any and all Enhancements required by federal or state governmental, or professional regulatory mandates related to UC's use of the Services; and (c) the Documentation associated with any Enhancements.

- iii) Supplier will provide Enhancements to UC upon their general release and no later than the time when the first five percent (5%) of Supplier's customers receive those Enhancements.
- iv) Except as otherwise provided in a signed addendum to this Agreement, nothing herein will obligate Supplier to enhance the Services in any particular respect or on any particular date. The decision as to whether and/or when, to enhance the Services will be within Supplier’s discretion.
- h) Spirion will provide a review of product road map updates when requested by the UC System.

7. Purchase Order

- a. Unless otherwise provided in this Agreement, Supplier may not begin providing Services until UC approves a Purchase Order for the Services.
- b. Any purchase by any UC location of the Services included in this Agreement will be covered by the terms of this Agreement.

8. Pricing

- a. The Services will be available for UC purchase, at UC’s sole discretion, during the term of this Agreement as stated herein.
- b. Supplier will sell the Goods and Services under this Agreement through their reseller, SHI Inc (“Reseller”) and payment terms shall be as agreed to between UC and Reseller.
- c. Supplier will partner with Reseller to pass through to UC all pricing and discounts as stated in Exhibit 2_Pricing Sheet, attached to the SOW (Attachment A to this Agreement), however, Reseller may offer additional incentives at their sole discretion.

9. Notices

As provided in the UC Terms and Conditions of Purchase, notices may be given by overnight delivery or by certified mail with return receipt requested, at the addresses specified below. Additionally, notices by Email will be considered legal notice if such communications include the following text in the Subject field: FORMAL LEGAL NOTICE – [insert, as the case may be, Supplier name or University of California].

To UC, regarding confirmed or suspected Breaches as defined under Appendix – Data Security and Privacy:

Name	Monte Ratzlaff		
Phone			
Email	Monte.Ratzlaff@ucop.edu		
Address	1111 Franklin Street, Oakland, CA 94607		

To UC, regarding Breaches or Security Incidents as defined under Appendix – Business Associate:

Name	Noelle Vidal		
Phone			
Email	Noelle.Vidal@ucop.edu		
Address			

To UC, regarding contract issues not addressed above:

Name	Bala Balakumar		
Phone	310.794-6012		
Email	Bala.balakumar@ucop.edu		
Address	1111 Franklin Street, Oakland, CA 94607		

To Supplier:

Name	Scott Giordano		
Phone	408-620-5482		
Email	Scott.giordano@spirion.com		
Address	200 Central Ave., Ste. 1900, St. Petersburg, FL, 33701		

10. Insurance

Supplier must deliver the Certificate of Insurance to UC's Buyer by mail or overnight delivery. Additionally, this requirement will be considered satisfied if a PDF version of the Certificate of Insurance is sent by Email and includes the following text in the Subject field: CERTIFICATE OF INSURANCE – Spirion

11. Service-Specific Provisions

- a. Additional Warranties:
 - i. Goods and/or Services Warranty. Supplier represents and warrants that the Goods and/Services provided to UC under this Agreement will conform to, be performed, function, and produce results substantially in accordance with the Documentation. Supplier will offer UC warranty coverage equal to or greater than that offered by Supplier to any of its customers.
 - ii. Third Party Warranties and Indemnities. Supplier will assign to UC all third party warranties and indemnities that Supplier receives in connection with any Services provided to UC. To the extent that Supplier is not permitted to assign any warranties or indemnities through to UC, Supplier agrees to specifically identify and enforce those warranties and indemnities on behalf of UC to the extent Supplier is permitted to do so under the terms of the applicable Third Party agreements.
 - iii. Date/Time Change Warranty. Supplier represents and warrants to UC that the Services provided will accurately process date and time-based calculations under circumstances of change including, but not limited to: century changes, daylight saving time changes, leap year changes and leap second changes. Supplier must repair any date/time change defects at Supplier's sole expense.

12. Cooperative Purchasing

Supplier agrees to extend the terms of this Agreement to Participating Agencies (public and private schools, colleges and universities, cities, counties, non-profits, and all governmental entities) registered with OMNIA Partners, Public Sector. All contractual administration issues (e.g. terms and conditions, extensions, and renewals) will remain UC's responsibility except as outlined in the above referenced Request for Proposal "RFP 02197-SEPT2020 – UC Systemwide RFP for Information Technology Security Tools." Operational issues, fiduciary responsibility, payment issues, performance issues and liabilities, and disputes involving individual participating agencies will be addressed, administered, and resolved by each Participating Agency.

13. Amendments to UC Terms and Conditions

The University of California Terms and Conditions of Purchase (04/05/21) are hereby amended as follows:

The University of California Terms and Conditions of Purchase (04/05/21) are hereby amended as follows:

- a) Article 2D: Is deleted in its entirety and replaced with " UC may by written notice terminate the Agreement for Supplier's breach of the Agreement, in whole or in part, at any time, if Supplier refuses or fails to comply with the provisions of the Agreement, or so fails to make progress as to endanger performance and does not cure such failure within ten (10) business days, or fails to supply the Goods and/or Services within the time specified or any written extension thereof. In such event, UC may purchase or otherwise secure Goods and/or Services and, except as otherwise provided herein, Supplier will be liable to UC for any excess costs UC incurs thereby.
- b) Article 4: Is deleted in its entirety
- c) Article 6A (vi) is deleted in its entirety and replaced with new Article 6L as follows: Spirion warrants that the Software, if installed and operated in accordance with the Documentation, will perform substantially in conformance with the Documentation, for a period of six (6) months provided that Licensee has installed all Maintenance Releases previously made available to Licensee
- d) Article 6D is deleted in its entirety and replaced with "As applicable to the Supplies and/or Services being provided under the Agreement, Supplier warrants that:
 - 1. It will comply with California and federal disability laws and regulations; and
 - 2. Supplier in a timely manner to respond to remediate to any identified accessibility defects in the Goods and/or Services to conform to WCAG 2.0 AA; and
 - 3. Supplier agrees to in a timely manner respond to and use reasonable efforts to resolve and remediate any complaint regarding accessibility of its Goods and/or Services
- e) Article 6J: Delete the second sentence that begins with Additionally and replace it with "Supplier warrants that no work will be performed under the Agreement with workers from those countries as listed at <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information> except as described in Supplier's bid.
- f) Article 7A: Is deleted in its entirety
- g) Article 8: Add a new paragraph at the end as follows: Limitation of Liability. EITHER PARTY'S ENTIRE LIABILITY AND THE OTHER PARTY'S EXCLUSIVE REMEDY FOR DAMAGES ON ACCOUNT OF ANY CLAIM ARISING OUT OF AND NOT DISCLAIMED UNDER THIS AGREEMENT SHALL BE: TO THE EXTENT PERMITTED BY LAW, THE TOTAL LIABILITY OF EACH PARTY ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PRODUCTS AND SERVICES HEREUNDER WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, SHALL NOT TO EXCEED, ON A PER CLAIM OR AGGREGATE BASIS DURING ANY TWELVE (12) MONTH PERIOD, AN AMOUNT EQUAL TO THREE (3) TIMES THE NET CHARGES INCURRED BY CUSTOMER FOR THE AFFECTED SERVICE DURING THE TWELVE (12) MONTHS PRECEDING THE MONTH IN WHICH THE CLAIM AROSE
- h) Article 9E: Delete in its entirety
- i) Article 9F (e): The fourth P3 and P4 entry is deleted and replaced with " Article 9F(e), fourth entry is amended to read: P3 and P4, 70,000 or more records - this insurance policy must have minimum limits of \$5,000,000 each occurrence and \$5,000,000 in the aggregate.
- j) Article 24: Deleted in its entirety
- k) Article 25: Deleted in its entirety
- l) Add a new Article 40 as follows: Arbitration. "Any dispute, controversy, or claim arising out of or relating to the Agreement,

or the interpretation, enforceability, performance, breach, termination, or validity thereof, including, without limitation, this arbitration clause, may be settled by confidential arbitration in Oakland, California, in accordance with the Commercial Arbitration Rules of the American Arbitration Association. Any neutral arbitrator appointed pursuant to this Section must be selected by mutual agreement of the parties or their appointees and shall be a JAMS approved arbitrator. An award rendered in connection with arbitration pursuant to this Section shall be final and binding upon the parties, and any judgment upon such an award may be entered and enforced in any court of competent jurisdiction. No provision of this subsection limits the rights of a party to the Agreement to obtain provisional, injunctive, or ancillary remedies from a court of competent jurisdiction before, after or during the pendency of any arbitration. Neither party has the right to arbitrate on a class action basis any dispute, controversy, or claim arising out of or relating to the Agreement, or the interpretation, enforceability, performance, breach, termination, or validity thereof, including, without limitation, this arbitration clause.”

14. Incorporated Documents

The following documents are incorporated and made a part of this Agreement by reference as if fully set forth herein, listed in the order of precedence following the Agreement:

- a) Statement of Work – Attachment A
- b) UC Terms and Conditions of Purchase, dated 4/5/2021
- c) UC Appendix – Data Security and Privacy, dated 8/12/19;
- d) UC Appendix – Business Associate, dated 8/2/2019

The terms of the documents below are applicable only to the extent they do not conflict or are not inconsistent with a), b), c), d) above

- e) Spirion Customer Support Services and Service Level Agreement – Attachment B
- f) Software As A Service Terms – Attachment C
- g) Spirion Software License Terms – Attachment D

15. Entire Agreement

The Agreement and its Incorporated Documents contain the entire Agreement between the parties and supersede all prior written or oral agreements with respect to the subject matter herein. No click-through, or other end user terms and conditions or agreements (“Additional Terms”) provided with any Services or products hereunder will be binding on UC, even if use of such Services or products requires an affirmative “acceptance” of those Additional Terms before access is permitted. All such Additional Terms will be of no force and effect and will be deemed rejected by UC in their entirety.

The Agreement is signed below by the parties’ duly authorized representatives.

**THE REGENTS OF THE
UNIVERSITY OF CALIFORNIA**

SPIRION, LLC

DocuSigned by:

Thomas Trappler

303F2BA33D81455...

(Signature)

Thomas Trappler

(Printed Name, Title)

11/4/2021

(Date)

DocuSigned by:

Tom Palomaki

A7D8661FC1BA423...

(Signature)

Tom Palomaki

(Printed Name, Title)

10/29/2021

(Date)

Attachment A to Purchasing Agreement ##2021003177

UC Statement of Work

1. Description of the Scope of Services:

The purpose of this Statement of Work is for Supplier to provide the University with Data Detection tools (including as applicable Professional Services) and related tools Goods and Services, in a cost effective and efficient manner, accompanied by high standards of quality and service, aligned with University's needs as further detailed herein.

Prior to any engagement between the University and the Supplier, a UC location specific Statement of Work referencing the terms of this Agreement shall be negotiated between the UC location (s) and Supplier outlining all key tasks and work activities including but not limited to: discovery, migration, implementation plan and timeline, additional SLAs, deliverables/milestones, payment schedule, key personnel, assumptions, obligations of each party, change process and acceptance criteria and testing.

The effective date of the term of any Goods and/or Services acquired under this Agreement shall be the date the UC Location has approved that the Goods and/or Services are fully functional in a production environment.

Supplier must provide the necessary staff, infrastructure, and other resources at a level sufficient to ensure efficient, effective, and continually improving fulfillment of its obligations under this Agreement. Supplier's provision of the Goods and/or Services must always be in a manner and level equal to or greater than as detailed in Supplier's Response to the UC RFP 002197-SEP2020 – UC Systemwide RFP – Information Technology Security Tools ("RFP") which is attached as Exhibit 1 the Statement of Work.

2. Participating Locations

Supplier shall make all terms of the Agreement available to all current and future locations of the University of California and its Affiliates as further detailed at <https://www.universityofcalifornia.edu/uc-system/parts-of-uc>.

3. Sustainability:

Supplier will register and participate in an assessment of their sustainability practices and procedures through the EcoVadis Corporate Social Responsibility (CSR) monitoring platform. For more information on the EcoVadis platform and costs associated with an assessment, please see the EcoVadis Supplier Solutions Website here: <https://www.ecovadis.com/us/supplier-solutions-2/>.

4. Pricing:

During the Initial Term and any subsequent Renewal Terms, the prices of Supplier's Goods and Services in Exhibit 2 shall not increase.

5. Supplier Implementation

5.1 Exhibit 3 to SOW: Spirion Implementation and Training & Services

Exhibit 1 to Statement of Work

Spirion's response to the UC RFP 002197-SEP2020 – UC Systemwide RFP – Information Technology Security Tools (Data Detection & Classification category)

Table 1 Supplier Capability

1	Are you a manufacturer (OEM), Value Added Reseller (VAR), or distributor?	Manufacturer
2	Is the OEM going to submit the response to this RFP directly and be responsible for fulltime and distribution of the product(s)?	Yes
3	If the OEM is going to submit the response to this RFP with coordination and collaboration with a channel partner for fulfillment and distribution of the product(s), the UC requires a Master Agreement with the OEM in addition to a purchasing agreement with the channel partner. Please acknowledge your acceptance of this requirement.	Yes. Spirion will be partnering with SHI on this response. Spirion will execute a Master Agreement with Univ. of CA upon award. SHI will be responsible for Fulfillment only. SHI is already an Omnia Partner.
4	If a VAR/Channel partner is going to submit the response to this RFP with coordination and collaboration with an OEM with the channel partner for fulfillment and distribution of the product(s) attach a letter of attestation signed by the OEM stating the nature of the collaboration	N/A
5	Please describe your company's capability of providing full service to all UC Locations. Describe your distribution model, including the size and location of your company's distribution facilities, warehouses and retail network.	The Spirion solution is software based. Fulfillment occurs via software license distribution. There is no need for distribution facilities, warehouses or retail networks.
6	Will your company's employees who are responsible for providing Services to your customers conform to the following? If so, please describe: Carry Picture ID, have passed background security checks?	Yes. All Spirion employees must pass a background check at the time of hire.

7	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. Include attachment if necessary	Sr. Account Manager handles all pre-sales inquiries and directs to the appropriate teams. Systems Engineer who assists with pre-sales assessments. Professional Services team with a project manager and engineer to help ensure successful implementation. Following implementation a Customer Success Manager will take over the account and assist with all activities from updates on products, support and renewals.
8	If you are a VAR or distributor, what is the average response time for an account manager(s) to respond to initial requests?	>4 hours
9	Identify any partners, subcontractors or any other staff/personnel resources outside of your company that you are partnering to perform the Goods and/or Services contemplated under this RFP and the role they play in performing the Goods and/or Services.	Spirion will be partnering with SHI for Contract fulfillment ONLY. Spirion personnel will deliver all Professional Services associated with this contract.
10	Please specify your company's normal business hours in Pacific Time zone format for receiving orders and providing customer service including maintenance support both during and after normal business hours.	8-5 PT weekdays
11	Describe your quoting process and how you will meet our requirement of providing assistance with product sales questions, technical inquiries and customer service inquiries	A customer will have 2 contacts they can reach out to for assistance with quotes, getting technical questions directed or other inquiries. Additionally, we have a website where customers can submit questions as well as chat with a representative realtime.
12	Explain how your company proposes to resolve any complaints, issues or challenges. Please detail your company's problem resolution and escalation process for customer complaints and concerns.	Customer escalations can be submitted via Customer Success, Professional Services or the Account Team. The escalation is assigned and tracked during regular reviews. Customer updates and communication occur as frequently as needed to demonstrate advancement.

13	Describe your ability to regularly provide electronic reports (in Microsoft Excel and other formats) providing a wide range of information related to the resulting agreement at both the UC-wide level and for each individual UC location including, but not limited to quarterly usage reports. Data provided in the reports should include, but not be limited to: UC Location, UC Department, UC Purchase Order Number, Name and Model of Service(s) purchased, usage volumes, discount percent, MSRP, UC final discounted price, price paid, per unit and total	Usage information can be captured through the console and exported as needed.
14	Describe what else your company will do to support UC's overall mission during the term of the agreement? UC's mission statement is available at: https://www.ucop.edu/uc-mission/ .	Spirion focuses on protecting what matters. We build and deliver the most accurate data discovery.

Table 2 Supplier Support

1	Describe all maintenance and support packages, and summarize the services, deliverables and terms included (for example, bug fixes, patches, service packs and associated services).	Spirion has a quarterly release cycle and occasionally a dot release as needed to address cloud api changes and/or bug fixes. These releases are full installs.
2	How is the customer notified for vulnerabilities or patch updates?	The Spirion SDM console provides notices of new releases
3	Do you have a development team that is responsive to new feature requests?	Yes
4	Describe your upgrade process (include communication points and lead-time notification). Identify if it is a re-implementation.	Spirion SDM upgrades are performed by the organizations Spirion Administrator. Installs are run on top of existing installations and require no downtime.
5	Can upgrades be deferred and schedule as needed?	Spirion SDM upgrades are installed by the organization's Spirion Admin and such can be done at any time or skipped if desired.
6	Is there a Technical Account Manager assigned to the portfolio for escalations?	Official Spirion Technical Account Managers can be assigned for an additional cost. Customer Success Managers are assigned to every customer.
7	Describe geographical location and structure of your support team.	All Support personnel are US based and located in central Florida
8	Is support available via telephone, email, remote access.	Support is available via web or email created tickets. Telephone support may be purchased for an additional cost. Remote support is offered on a case by case basis
9	Describe support plan options, including general service level commitments offered under this support agreements.	Support is available from 7am to 6pm, Monday through Friday (excluding US Holidays). Ticket first response for critical issues is 1 hour. Ticket first response for non-critical issues is 4 hours.
10	Is support available via telephone, email, remote access.	Support is available via web or email created tickets. Telephone support may be purchased for an additional cost. Remote support is offered on a case by case basis
11	Describe the use of internet-based support of the solution including knowledgebase and technician access (online chat).	Spirion has a robust online knowledge base, online video training (growing every week), online user forums and online ticket creation. Support does not currently have online chat.

12	Describe service level response times during regular support hours as well as levels of support outside of regular support hours. The response should include by Severity Level the number of hours within which a response can be expected for non-emergency and emergency (production-down) inquiries. In addition, the response should define the duration within which a resolution is expected - for both non-emergency and emergency (production down) inquiries.	Support is available from 7am to 6pm, Monday through Friday (excluding US Holidays). Ticket first response for critical issues is 1 hour. Ticket first response for non-critical issues is 4 hours.
13	Do you offer stand-up meetings to go over progress, questions, feedback etc.?	Stand-ups if needed can be coordinated with your Customer Success Manager
14	Do you have a training catalog and curriculum available for selection at the customer's discretion	Yes Spirion's Customer portal has a growing selection of self-directed training - this is not currently a substitute for Spirion's Professional Services' training

Table 3 Technical Response - Data Detection

1	Does your solution offer all features, functionalities and capabilities asked in this questionnaire within a single product or does it require purchase of multiple products?	Spirion provides a first in class data detection tool
2	Provide name and version of all the product(s) listed in question 1	Sensitive Data Manager 11.7 or Data Privacy Manager 2.1
3	Describe the vision and direction for the products in this category	SDM is a on prem version and DPM is a SaaS version of our tools. Both have the same ability to scan and fins sensitive data with-in the most repository locations. Including but not limited to cloud, end points, databases, shares, and more. We also have a full OCR ability built in.
4	List your top five technology alliances with information technology vendors in this category	Bitglass, Tonic, McAfee, Microsoft
5	Describe your product differentiators versus other competitive products in this category	Less the 2% faults positives, Wides depth and breath of file types and locations. OCR capabilities. End Point device data detection and classification. Injection of metadata (GUID) classification into file Metadata. GIEDs can be read by SIEM, CASB, DLP, NGF, and other edge protection devices.
6	List all license models (example: On Prem, SaaS, Perpetual, Term) offered for the product(s) you are quoting in this category	We have both a on Prem and SaaS solution, but the license models are the same. We license either lifetime or subscription.
7	List and describe any related products and services not included in this Request for Proposal that your firm can provide that may be of benefit to the University. (See IT Security Price file in Pricing Questionnaire for instructions on providing pricing)	compliance (a tool used for subject access rights management). Analytics (a tool for breach detection and notification) Attached Files : Attach A1 & A2 Data_Sheet_DPM_Scalability_and_Scanning.pdf;SDM_DP M_Playbooks_Data_Sheet_Final.pdf
8	Provide information (including but not limited to architecture/strategy/planning/installation/configuration) on your implementation packages as a part of rolling out your product solution	See attached data sheet Attached Files : Attach B Spirion DPM Software Product Description (1).pdf
9	If offered, is pre-project planning support as part of enterprise engagements?	Yes pre-project planning and support are provided as part of our professional services options.

10	What is your implementation methodology in an organization with 10k+ employees?	Our methodology starts with a conversation with the client stakeholders to build out a statement of work.
11	Do you offer your discovery products as a hardware appliance , SaaS, or Software that can be deployed on premise.	Spirion's tool as stated above comes in 2 flavors SDM (on Prem) or DPM (SaaS)
12	List supported operating systems for agents	Windows, MAC and RHEL
13	Endpoint scanning: Does your solution support agent or agentless scanning	Spirion's tool supports end point deployed directly on a device. Or we can also do remote scanning of devices like network shares, DB, exchange and more would use either 1 or many endpoints that remotely credential to the repository.
14	List supported OS Management Console:	SDM used Windows 2012R2 or newer. DPM is SaaS so N/A.
15	Scanners: List the OS that can be hosted	SDM is Windows self-hosted tool (Windows 2012R2 or newer) DPM is a Spirion SaaS hosted solution
16	Does the product support IPv6	Spirion's tools both SDM and DPM support IPv6
17	Does the product allows deployment using a distributed architecture to bypass ACLs, firewalls	Agent deployment can be deployed using your current methods for MSI Deployment.
18	Can your product export scanning results via XLSX, XLS, CSV, PDF, any connection to a RESTful API	We can export to either CSV or PDF
19	Are notifications delivered to appropriate roles so that they can take action according to the analysis or notification delivered.	Notifications can be set up on a per workflow bases for targeted visibility or action
20	Describe your product's ability to email reports (scheduled and ad-hoc)?	Reports can be send when a notification is sent (new data detected), or on a schedule, or even ad-hoc
21	Does your solution have configurable email alerts?	Yes Spirion's Email alerts are very configurable
22	Can your product create and audit eDiscovery cases/investigations	Yes, our tool can be used to provide assistant in the case of breach or eDiscovery investigation

2 3	Does this product support Role-Based Access Control (RBAC)	Spirion can remove permission on files that contain sensitive data, and also provide ACL information
2 4	Does your product support data visualization, including object relationship mapping?	DPM and SDM do not provide the relationship mapping, however with the Compliance add-on we do provide this level of relationship
2 5	Does your product have a detailed object/investigation report generation?	Spirion provides the location, file name, and the type of data within the file
2 6	Does your product have Metadata reporting?	Spirion can report the metadata of the files
2 7	Describe your product's integration with Active Directory	Spirion can do an LDAP read of your AD and thus provide used the ability to login with AD credentials
2 8	Does your product allow for integration with SIEM that allow for results exceeding a threshold to be sent	Spirion's GUID can be read by a most of SIEMs either with a direct GUID input or a regex
2 9	Describe your product's support for multiple protocols for single sign on (ex. CAS, SAML, OAuth, OpenID)	Spirion supports SAML 2.0 for SSO
3 0	What are the Data Types Supported	Spirion has a number of out of the box Anyfind technology and then we also support keyword, dictionaries, phrases, regex, IP, and more depending on the level of complexity you would like to use.
3 1	Are chat logs (such as MS Teams, Slack) supported	Some Teams chats are captured via SharePoint and OneDrive. Other are on the RoadMap
3 2	List Cloud file storage supported including but not limited to Box, OneDrive, Google Drive	Spirion supports O365, Dropbox, OneDrive, G-Suite, Box
3 3	List Cloud-object-storage supported including but not limited to Amazon S3, Azure Blob Storage, Google Cloud Storage	Spirion supports Amazon S3. Azure Blob, Redshift data lakes, Avro, and others are road mapped
3 4	Describe your support for Email platforms — Exchange, Exchange Online, Gmail, IBM Notes, any generic IMAP server	Spirion supports exchange local, exchange in O365, Gmail, Thunderbird, Lotus Notes, OST, PST.
3 5	List all the network files systems supports.	Spirion supports CIFS, SMB, SAMBA, DFS

3 6	List the databases supported for scanning	Spirion supports MS SQL, No SQL, Oracle, DB2, Postgress, Informix, Sybase, SQLbase, SQL anywhere, SQLite, Access, Interbase, Azure DB, Other DBs via ODBC, MongoDB
3 7	List the document/content management systems for scanning	Generally, if you can provide Spirion access rights to the system we can scan it.
3 8	List the file systems supported (e.g. NTFS, APFS, ZFS, etc.)	Spirion supports many file types (more than 100 types)
3 9	Does your tool Scan Azure?	Spirion SDM can scan or even be hosted in Azure. DPM is hosted in an Azure tenet
4 0	Does your tool Scan data locally?	Spirion does support local scanning
4 1	Does your tool Scan data on a remote device?	As stated above Spirion can scan remote shares or machines with the appropriate credentials
4 2	Does your Scan data on AWS?	Spirion's SDM can be hosted in AWS and can also scan AWS. DPM can scan AWS.
4 3	Does your tool Scan Google Cloud Apps	We currently scan Gmail and G-Drive. We are a data at rest scanning tool.
4 4	Does your tool scan common SaaS applications, such as Salesforce, ServiceNow and Workday	Spirion currently recommends a backup copy of the data be created for scanning vs a direct connection right now. We are working on a direct connection on our roadmap.
4 5	Describe your product's ability to import custom data dictionary/custom signatures?	Spirion can use customer dictionaries, keywords, phrases, or regex
4 6	How does your product mask scanning results	This question depends if you mean in the tool (then the findings are only exposed to users with the correct level of access), if you are referring to the DB for storage then it is all encrypted, if you are asking about the findings in the documents then Spirion can do redaction on writable files.
4 7	Can your product run scheduled scans	Spirion's tools can run either Sd-Hoc or set to scan on a schedule
4 8	Does your tools have the ability to tune based on rules of proximity?	Spirion's tools are very customizable for location and even targeted directories
4 9	Does your product allow for users to login to the console to see only their results?	Depending on how the tool is configured and the permissions of the user we can customize the results provided.

50	Can your product run network scans?	Spirion can scan across the network but does not scan network hardware. We are a Data at rest solution
51	Can your product run On-Demand scans?	Spirion's tools can run either Sd-Hoc or set to scan on a schedule
52	Does your product "throttle" the scans to minimize impact	Spirion's tool has the ability to tune the endpoints for CPU, memory, IOPS and more.
53	What detection and classification techniques does your product's agent based scanning support	Spirion uses our own data science behind our Anyfind technology along with other customer needed information to find sensitive data for either local or remote scanning
54	What detection and classification techniques does your product's remote based scanning support	Spirion uses our own data science behind our Anyfind technology along with other customer needed information to find sensitive data for either local or remote scanning
55	Please provide the type of discovery scanning you support (e.g., full, differential or partial repository sampling).	Spirion completes a full scan first and then can do delta scans once the full scan is complete
56	What is your recommended discovery scan policy for different repositories/use cases?	This would be something we would work with the customer to customize based on the speed, type of data, and other factors when we for a Professional Services scoping call and Scope of Work.
57	Provide details on discovery performance in MB/GB/TB scanned/hour (describe assumptions and architecture).	Spirion stated 1 GB/agent per hour. This is an average based on the full allotment of file types including files that need to be scanned using the OCR engine. However we do have ways to increase the scan time with some tuning that we cover during the PS scoping call
58	Describe your tool's automatic classification of discovered data	Spirion uses a workflow to identify the data types and then apply classifications to the documents that meet the rule set
59	Describe the ability to be able to flag false positives so the scanning tool can learn	Spirion's tool is based on static rule sets. If the customer identifies a faults positive we can look at why and take corrective action.
60	List all the pre-defined templates can you provide?	Spirion has the out of the box Anyfinds (see attached to question 7) and then also has a number of included other types of finds (approx 200) to use. Along with any custom ones needed during the Spirion PS engagement
61	Do you provide ML capabilities for IP data identification?	Spirion has a great deal of experience with IP and has found that in the past ML has not been as good at identifying IP as our static rules that the PS team can configure for you
62	Does your tool have the ability to tag or otherwise mark an object with metadata to enable actions or	Spirion writes a unique GUID into the Metadata of the file that is readable by other edge devices

	decisions to be made? If yes, please describe the manner in which this is accomplished.	
6 3	Does the product have the ability to embed a file or object with metadata	Spirion writes a unique GUID into the Metadata of the file that is readable by other edge devices
6 4	How does your product support automated rules based classification	Spirion's tool does all classification with in our workflow portion of the tool
6 5	How does your product support User-based Classification	Spirion has a few ways the user can classify. They can right click and from the properties menu classify, they can classify from with-in the Office or Adobe Suite or they can classify with in the console tool
6 6	A researcher moves data containing PHI from the appropriate data escrow to another institution-managed device. The data is then exfiltrated from the environment.	If properly configured the user should not be able to move the file to a non-authorized location based on edge devices watching for the GUID within the Metadata. Spirion is a data at rest solution.
6 7	An employee saves customer credit card information in plain text on their desktop. The file is then backed up to a shared drive which is readable by multiple users.	Spirion has a tool that is included called File Watcher that can be configured to watch the end users machines and watch for data types and then based on a rule could take action once the file is saved. For example: Saved credit card brakes the rule of save to the desktop, first redact the CC information and then quarantine it to a save location for further action.
6 8	Identifying and classifying structured data such as passport numbers, social security numbers, payment card numbers, student IDs, employee IDs etc.	Spirion can find and report on the sensitive data defined in the tool. If you want to provide remediation action within structured databases we partner with Tonic to de-identify the information.
6 9	Sensitive financial reports are misclassified in a shared drive. Multiple employees report viewing the information and are upset by the content.	Depending on how and what was created this would only happen if a rule was not created to find and protect this information. Otherwise this would have already been classified correctly. If for some reason it was wrongly classified this would be handled like a fault positive or faults negative.
7 0	Identifying and classifying unstructured data such as ITAR research information	Spirion's tools are based on rules and thus can have them built around ITAR or any other compliance needs
7 1	An institution may be audited for regulatory compliance (GDPR, HIPAA, PCI, and other standard applicable to UC), describe how your product can help demonstrate compliance to an auditor.	Depending on what products you select from the Spirion portfolio we help with a data inventory, relationship association, point in time reporting, and more

7 2	The university is managing a legal investigation and an investigator needs search for content matching a specific signature. Explain how your product would enable the investigator to provide this evidence.	Spirion's OCR engine also can do hand writing for signatures, or add this to other Anyfind technology to help add additional complexity.
--------	---	--

Scalability and Performance with Spirion Data Privacy Manager

Achieve Privacy-Grade data discovery and purposeful classification in a highly scalable SaaS hybrid architecture that can thoroughly scan both on-premises endpoints/servers and cloud repositories.

Problems with Traditional Scanning Approaches

Traditional data discovery scans can be time consuming in order to yield accurate results. Most approaches choose to sacrifice accuracy, omit certain locations, and miss context in order to “complete” discovery quickly. These design choices don’t result in thorough discovery as they yield false positives – or even worse, false negatives, leaving gaps in location coverage. This fails to provide the depth of information required to understand the context of the data found resulting in concerns over accurate compliance with privacy regulations.

Bandwidth, Capacity, and Contention

Bandwidth and capacity are also a concern due to the high volume of data being read during scans. To compensate, it is important to keep the scanning software or agent as close to the data as possible, thereby greatly reducing bandwidth requirements and avoiding contention with other users.

Agents vs Agentless, or Both?

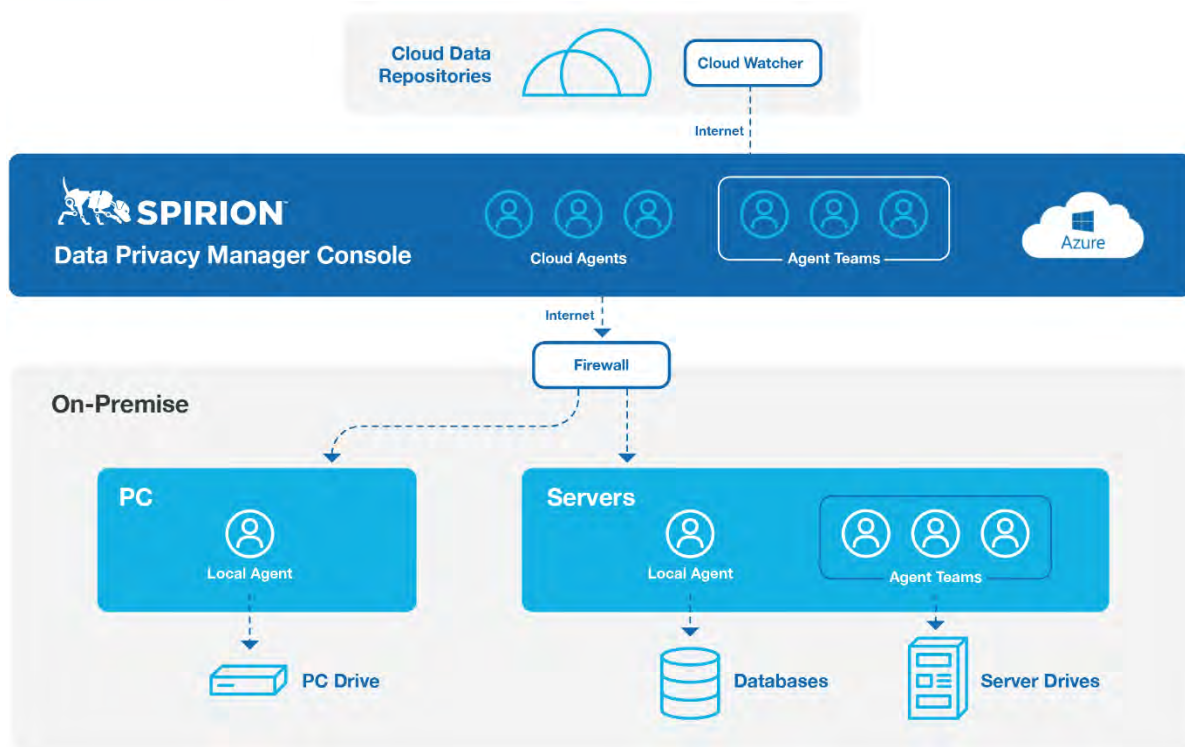
Some other discovery solutions offer only agentless scanning, where all data is read by a single centralized deployment of cloud-based software.

While this centralized approach can be simpler to deploy and maintain, it may also have significant limitations and performance issues if on-premises drives or databases need to be scanned for compliance or security reasons, including:

- Network contention and congestion on internal LANs, across firewalls, and during transit of Internet connections.
- Consumption of excessive Internet bandwidth needed by other critical functions like off-site backups and other SaaS applications.
- Significant cloud repository egress fees may be incurred when data is scanned in a cloud repository without using an agent within or directly adjacent to the cloud repository.

The Solution

Spirion Data Privacy Manager (DPM) allows for agent-based, agentless or a hybrid combination for deployments. Local Agents can be deployed directly on servers and PCs where advantageous. Cloud Agents can be used to scan both repositories and or a combination of cloud and on-premises locations.



Cloud Agents

Cloud Agents run up in the cloud on the Azure platform. They work from a shared global search history, so they are aware of what other agents have already scanned. This eliminates duplicative rescanning while ensuring that a complete and thorough scan is done and the results are immediately visible in the DPM Console as the scan progresses. Cloud Agents can be automatically added or destroyed, and groups of Cloud Agents can be launched as an Agent Team wherever needed. This offers time and cost efficiencies with no pre-configuration overhead or dedicated hardware requirements.

On-Prem Agents

On-Prem Agents are usually deployed to on premise workstations, PCs, servers being scanned, or other local compute platforms. They make highly effective use of local compute resources and the high bandwidth/low contention storage busses connecting disk drives to the server or PC they are running on. Because only the scan results are returned to the DPM Console, On-Prem Agents greatly reduce network bandwidth and content issues.

Cloud Watcher

Cloud Watcher is a new feature that is like a Cloud Agent. Rather than performing scans on demand or based on a preset schedule, Cloud Watcher starts a new scan by a Cloud Agent whenever a cloud repository API indicates that new or changed data is present. This capability improves the performance and scheduling impact of scanning for new or changed data by only scanning when necessary.

Agent Teams

By combining sets of Cloud Agents or On-Prem Agents into an Agent Team, DPM can speed up large scans by breaking the work into small segments, allowing for distributed or parallelized scanning that greatly reduces overall scan times. Agent Teams are fully automated and highly scalable – you simply select a set of Agents to use and DPM figures out how to divide and distribute the scan process across them, sharing a global scan history to ensure that no work is duplicated. As additional Agents configured for the scan become available, they check a queue for the next available scan portion and begin scanning immediately.

Hybrid Architectures provide Flexibility, Scalability, and Performance

Asking whether a discovery tool is Agent-based or Agentless/Centralized is asking the wrong question. The question should be – what method is best for the organization? Usually the answer is a combination of both Agent-based and centralized scanning in a hybrid approach to provide both flexibility and scalability. Data Privacy Manager offers choice in deploy agents where necessary while still providing robust centralized, automated, and highly scalable agentless scanning options for consistently high performance and comprehensive discovery. Data Privacy Manager allows for the use of the method that is most appropriate for the task at hand to avoid compromises and maximize the total cost of ownership.



Spirion Data Privacy Manager

Operational Efficiencies with Playbooks

Spirion's new Data Privacy Manager (DPM) provides industry-leading sensitive data discovery and classification in a highly scalable SaaS hybrid architecture, with the capability to thoroughly scan both on-premises endpoints/servers and cloud repositories for performance and protection.

Why a Playbook Matters

As well as being the watch dog of an organization's sensitive data, DPM uses Playbooks instead of workflows to help teams prepare for and handle incidents without worrying about missing a critical decision.

Unlike convoluted processes with other approaches, the easy-to-understand UI creates a step-by-step investigation. By following simple commands that allow for a remediation process with actions and weights at each step, users can stack multiple actions based on decision points that can also be prioritized for better decisioning.

Playbooks allow for fine grained control of sensitive information. This allows companies to handle the same types of data differently, as needed. Diverse sets of actions can be configured depending on a wide variety of information, from file location or access control lists to when files were last modified or accessed and by whom.

Playbooks are suitable for all users ranging from the most novice administrator to a seasoned analyst and are regulated by their on-access permissions. Since only approved actions can be taken at any step, potential errors and omissions in detecting and remediating data privacy risks are greatly reduced.

The DPM Playbook is a method to help teams match the complexity required by an organization to prepare for and handle incidents and overall simplifies complex tasks through automation to control sensitive data.

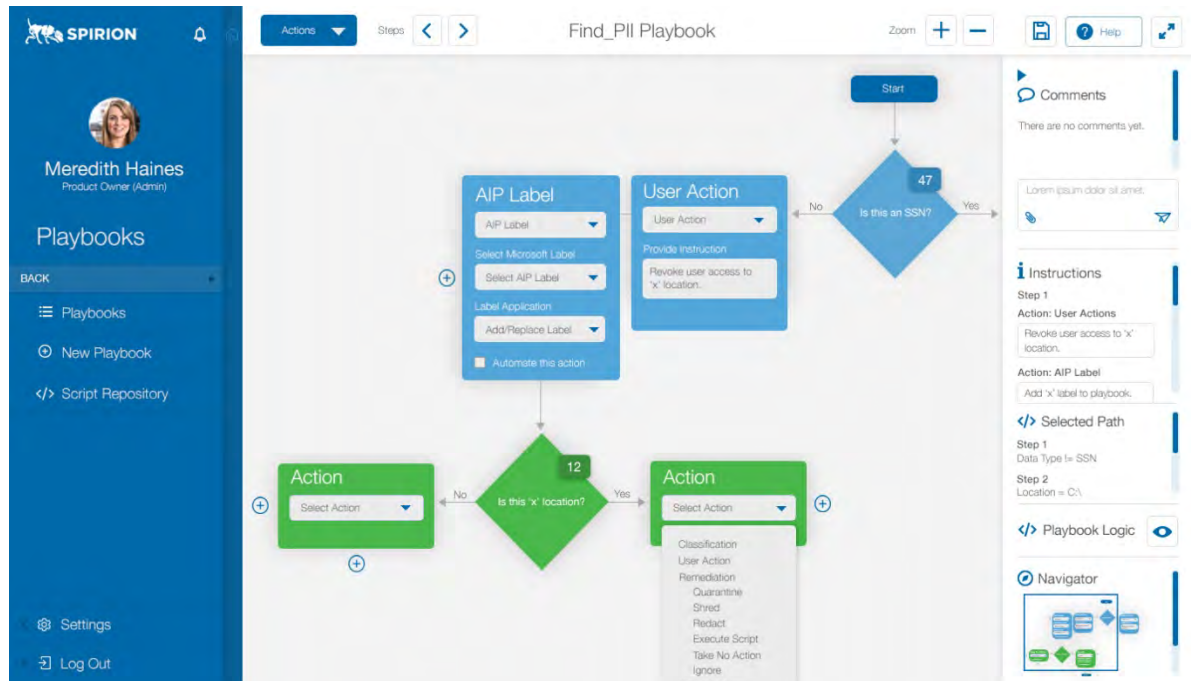
Playbooks vs Policies and Workflows in Sensitive Data Manager

The workflows in Sensitive Data Manager (SDM) provide the ability to assign results to users based on user defined criteria, send notifications when automatic or manual assignment occurs, apply remediation actions, track status and assign classifications. This provides a complete process for end users, However, SDM workflows are complicated to implement, design, and they aren't easily replicated.

By comparison, Playbooks takes and builds on SDM Workflows by adding vastly expanded conditional branching, approvals, notifications, and automation that offer ease of use and time efficiencies due to the inherent flexible design.

New UI that provides a delightful UX

DPM's new UI enhances the visual aspects of Playbooks making it easy to use with a sensible and trainable UI. Playbooks uses interactive cards that provide all relevant options while hiding everything irrelevant to the user's task at that moment. It uses progressive disclosure by adding single cards, one at a time in the Playbook builder, and uses self-segmentation in the Playbook viewer to empower the user to choose their own path through remediation.



This is better than SDM's workflows as it is easy to use with intuitive design flows that provide all possible options for remediations in a relevant, simplified UI that implements the concept of Playbook "cards". Users can access a simple dropdown configuration for details. Each set of cards represents an easy to follow colored path that is easy to differentiate from the path not taken that is greyed-out. Users can easily see the automated step progress for remediation with a status indicator, and a navigator that allows the user to conveniently traverse a complex flow.

Operational and time efficiencies are just a click away with Playbooks in Data Privacy Manager. Offer your data privacy team the much need protection and performance to handle incidents without missing a critical step.


SPIRION™
SOLUTION OVERVIEW

Spirion Sensitive Data Platform

The Challenge

Data proliferation, increased data protection and privacy legislation and data loss incidents are top of mind concerns for businesses today. Organizations are tasked with protecting their data footprint to address these challenges but find that it can be very difficult to protect sensitive data if you don't know what you do have or where it resides within the ecosystem. This lack of data insight puts organizations at risk for data breaches, reputational damage and fines for non-compliance with data protection laws.

The Solution

Spirion Sensitive Data Platform (SDP) provides Privacy-Grade™ data discovery and purposeful classification in a highly scalable SaaS hybrid architecture, able to thoroughly scan both on-premises endpoints/servers and cloud repositories at enterprise scale. It quickly and automatically discovers, classifies, and remediates almost any form of sensitive data or personally identifiable information (PII) anywhere on-premises, in the cloud, and on all endpoints.

Spirion SDP's accurate and comprehensive data discovery and automated classification are the essential first steps for controlling the sprawl of sensitive data and

are vital to ensuring accurate and timely compliance with expanding privacy laws and regulations.

Find any sensitive data, in any location

Spirion's unique, and proprietary AnyFinds™ in combination with our sensitive data definitions are built-in for key data types. These proprietary technologies in addition to traditional keyword, dictionary, and RegEx scanning combine to provide the most accurate data discovery in the industry and are provided out of the box without the need for ML training.

The platform provides a flexible hybrid approach to data discovery and classification with both software-based agents for on-premises servers or endpoints and agentless scanning in the cloud for simplicity, scalability, and performance. Supported data locations include a wide range of databases, data lakes, file types, and cloud repositories such as Amazon S3 Buckets. Searching anywhere is one of the specialties of the platform, providing wide coverage scanning within extensive data file types including: Office, PDFs, text, personal storage files, and other unstructured data formats like images. All this technology combined provides the ability to identify what needs protecting all over the ecosystem to apply the necessary controls.



Modern scalable architecture

Spirion SDP's advanced, Kubernetes containerized microservices software architecture ensures high levels of scalability and performance, with a cloud-hosted console for configuration and management using an intuitive and efficient UI.

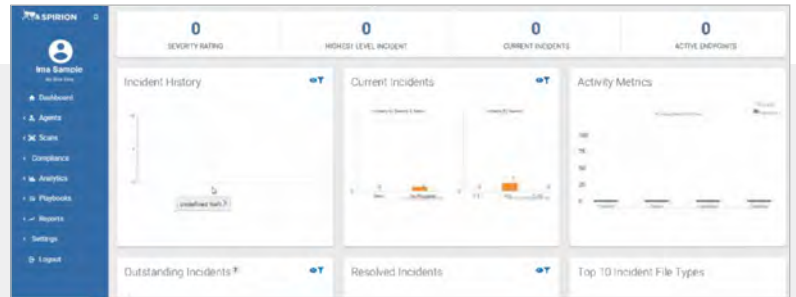


Modern Productive UI and Playbooks

Spirion SDP provides a modern User Interface (UI) with intuitive configuration tools like Playbooks. Wizards make it easy to step through even complex configuration steps. A real-time return of scan results allows quick tests of scheduled scans that run uninterrupted during off-peak hours. Playbooks use advanced interactive flowchart tools for a time efficient layout that allows for visualizing even the most complex sensitive data discovery, classification, and remediation workflows.

Advanced Dashboard and Flexible Analytics

Spirion SDP embeds Microsoft's Power BI engine for its advanced reports and dashboard visualizations, leveraging an enterprise-scale reporting and analytics engine already in use across the industry. Its dashboard provides both system-level overviews and an in-depth drill-down into sensitive data scan results to help organizations understand sensitive data within the context of their business.



Migrating from Sensitive Data Manager

Spirion SDP supports all of the use cases and data locations supported by Spirion's onpremises Sensitive Data Manager while providing cloud scalability and performance benefits, an improved UI and user experience, and faster time to value. Upgrading to

Spirion SDP is made easy with Spirion providing migration services, training, and support.

Spirion SDP is initially available as a secure SOC 2-compliant hosted solution on Microsoft Azure and will also be supported on Amazon AWS and private cloud or on-premises installations.

Secure the sensitive data at your enterprise with Spirion Sensitive Data Platform to apply the sensitive data controls and compliance that your organization needs.

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion has relentlessly solved real data protection problems since 2006 with accurate, contextual discovery of structured and unstructured data; purposeful classification; automated real-time risk remediation; and powerful analytics and dashboards to give organizations greater visibility into their most at-risk data and assets. Visit us at spirion.com

SPIRION IMPLEMENTATION SERVICES

CUSTOMIZED IMPLEMENTATION PACKAGE– PS-IMP-01



1. Overview

Proficiency and precision are necessary to effectively implement quality security solutions. To help you get the most out of the Spirion software (the “Products”), Spirion offers the following implementation services package (“Package”). This Package identifies some of the activities typically involved with the implementation of Products.

2. Deliverables and Responsibilities

2.1. Detailed Description of Services

Spirion employees, agents, and/or contractors (“Services Personnel”) will assist Customer with the performance of the following activities with respect to the Products in accordance with Spirion recommended engineering practices (“Services”): 2.1.1. Pre-Implementation

- Services kickoff call between Customer and Spirion Services Team to be scheduled within 7 days of order being processed
- Review scope of project
- Establish services schedule
- Confirm critical use cases
- Review technical requirements for implementation
- Confirm Customer’s designated Spirion Administrator and other team members

2.1.2. Standard Implementation

Services Personnel will assist the Customer with the implementation of the Product within one (1) Customer environment.

Installation

- Architectural consultation
- Console installation guidance/assistance
- Build agent deployment package(s)
- Install agent on one machine and test client/console communication

Configuration

- Import best practice policies
- Create and configure Discovery Team
- Interactive agent search testing
- AnyFind optimization
- Review available resources

2.1.3. Implementation Modules

Standard Implementation includes assistance with up to six (6) of the modules listed below. Additional modules can be added based on the Customer’s use case. For data stores, assistance includes configuration and testing of searches on a subset of each target repository in scope. The customer will

SPIRION – CUSTOMIZED IMPLEMENTATION PACKAGE – PS-IMP-01

be responsible for scaling these searches to full production. Each module includes scope limits specific to that target or activity.

Data Types (selected individually)

- Custom Simple Development/Optimization (up to 4)
- Custom Complex (1)

Target Types (selected individually)

- Windows Desktops (up to 10)
- Mac Desktops (up to 10)
- Linux Desktops (up to 10)
- Remote File Servers (1 DFS/NAS/server)
- Exchange (on-prem) (1 tenant, up to 10 accounts)
- Exchange (O365) (1 tenant, up to 10 accounts)
- SharePoint (on-prem) (1 site collection, up to 100 GB/sites)
- SharePoint (O365) (1 site collection, up to 100 GB/sites)
- Cloud Target (Box, DropBox, Google Drive, Google Mail) (1 target store, up to 10 accounts)
- Database (1 target, up to 10000 rows)

Custom Report Development (selected individually, may select multiple)

- Simple Custom Report (up to 4)
- Advanced Custom Report (1 up to 3 joined components)
- Deluxe Custom Report (requires DBE involvement, counts as two selections)

Workflows/Classification

- Creation and testing (up to 4)

Third-Party API/Integration Configuration

- Best Effort (up to 4 hours)

Consultation (e.g., one-on-one training or troubleshooting infrastructure)

- Up to 4, 1-hour sessions (subject to availability)

2.1.4. Functional Testing

Services Personnel will conduct post-implementation testing identified below in accordance with Spirion recommended engineering practices. A “Successful Implementation” will be determined by Services Personnel upon the occurrence, in Services Personnel’s reasonable discretion, of the items specified in “Functional Testing” attached hereto as Exhibit A including;

- Standard System and Architecture Overview
- System Navigation
- Discovery, Classification, and Remediation Policy Creation
- Basic Reporting
- Common Product issues and resolution

SPIRION – CUSTOMIZED IMPLEMENTATION PACKAGE – PS-IMP-01

- Relevant logs and debug options

Services Personnel will use commercially reasonable efforts to assist with the troubleshooting and correcting of obstacles identified during the Services. 2.1.5. Services Closure Meeting

- Service Personnel will conduct a Services closure meeting to review and confirm the Services have been completed and assist with the transition to Spirion Technical Support

Exhibit A: Functional Testing

Feature testing of the following will be limited to functional proof, typically involving either Yes/No or limited to two (2) elements of a particular attribute (for example: when running scans against target repositories and applying classification and remediation policies).

Standard Implementation	Result
Verify Spirion Console and Database installation	
Build agent deployment package(s)	
Verify Best Practice Policies imported	
Configure Test Search Policy	
Test Scanning (single agent)	
Build Discovery Team	
Verify Discovery Team Search	
Verify AnyFind Results	

Implementation Modules (as appropriate based on package selection)	Result
Build Custom Data Types	
Windows Desktops (up to 10)	
Mac Desktops (up to 10)	
Linux Desktops (up to 10)	
Windows Desktops (up to 10)	
Remote File Servers (1 DFS/NAS/server)	
Exchange (on-prem) (1 tenant, up to 10 accounts)	
Exchange (O365) (1 tenant, up to 10 accounts)	

SPIRION – CUSTOMIZED IMPLEMENTATION PACKAGE – PS-IMP-01

SharePoint (on-prem) (1 site collection, up to 100 GB/sites)	
SharePoint (O365) (1 site collection, up to 100 GB/sites)	
Cloud Target (Box, DropBox, Google Drive, Google Mail) (1 target store, up to 10 accounts)	
Database (1 target, up to 10000 rows)	

Implementation Modules (continued)	Result
Build Workflows (Classification and Remediation)	
Windows Desktops (up to 10)	
Mac Desktops (up to 10)	
Linux Desktops (up to 10)	
Windows Desktops (up to 10)	
Remote File Servers (1 DFS/NAS/server)	
Exchange (on-prem) (1 tenant, up to 10 accounts)	
Exchange (O365) (1 tenant, up to 10 accounts)	
SharePoint (on-prem) (1 site collection, up to 100 GB/sites)	
SharePoint (O365) (1 site collection, up to 100 GB/sites)	
Cloud Target (Box, DropBox, Google Drive, Google Mail) (1 target store, up to 10 accounts)	
Database (1 target, up to 10000 rows)	

Services Obligations of the Customer

Prior to the start of and throughout the Services, the Customer is required to have prepared resources as provided by the Services Personnel. Spirion requires an IIS Server, SQL Server, and Discovery Team Agent machines for implementation. Please review our technical and best practices guide for specific requirements. Service accounts are also needed for installation and authenticating to various target repositories to conduct scans. Details for the services accounts can be found in our Service Account Check List document. Both documents are available from your Customer Success Manager.

Additional pre-requisites include a list of the data types to be searched for, classification schema, and a remediation strategy if in scope.

Throughout the Services, the Customer will promptly provide all resources and licenses to Services Personnel to allow Services Personnel to deliver the Services.

Package Assumptions

- Services are delivered by remote delivery resources – No onsite delivery element.
- Services Personnel must receive a written cancellation notice at least twenty-four (24) hours prior to the start of any pre-scheduled Services
- Services will be provided during normal local business hours, Monday – Friday (e.g., 9:00am to 5:00pm)
- Services do not address any other products other than those licensed by Spirion to the Customer
- Services in this Package are limited and may not address all of the Customer’s unique requirements
- No High Level Design or Low Level Design documentation to be provided within this Package
- The Customer should not expect “ondemand” live support outside planned Services dates
- All scripts, tools, notes, know-how and procedures developed by Services Personnel as part of the Services will remain the property of Spirion
- Services Personnel will have no obligation to provide Services unless and until the Customer fulfills all of its Services Obligations
- The Customer’s current Support entitlement will be utilized for Product troubleshooting and escalation
- There is no report, memorandum, or other formal deliverable to be issued in connection with this Proposal.
- Spirion provides the Services “AS IS” and makes no warranties of any kind, express or implied
- Services will be performed in a professional manner, and Services Personnel will comply with all applicable laws in providing the Services
- Services must begin within 90 days of the Order or Subscriber forfeits the implementation Package
- Services must be completed within 6 months from the Order or 3 months from the first Services session following the Kickoff Call, whichever occurs first, or the Customer forfeits the implementation Package.
- The Customer’s assent to the Subscription Agreement constitutes acceptance of the above terms and conditions
- Any work or additional hours that, in Services Personnel’s reasonable discretion, exceed the scope of Services (including remote or onsite follow up work or troubleshooting unknown issues) will require a mutually agreed upon services contract
- Services and Deliverables within this Package are standard and non-negotiable

Terms & Conditions

- The Services in this implementation Package are provided pursuant to the Subscription Agreement.



Spirion Implementation and Training (SIT)

Description

The Spirion Implementation and Training (SIT) combines the best of online instructor-led training with Spirion Professional Services (PS) implementation assistance. Guided by the Spirion instructor, your Spirion administrator will learn the fundamentals of the application and have the chance to practice in a virtual lab. Then, Spirion PS will assist in designing and deploying your Spirion implementation.

Objectives

Classroom and Lab Objectives

Discover | Learn Spirion's best practices for developing, testing and executing searches against a variety of data repositories

Classify | Understand different methods of classifying your data and build your own custom classifications

Remediate | Practice quarantining, redacting, and shredding sensitive data in a safe lab environment

Production Implementation Objectives

Guide | Step-by-step assistance setting up and configuring Spirion in your company's unique environment

Discover | Assist your Spirion administrators with configuring, testing and fine-tuning search criteria against your data repositories

Report | Learn how to review search results, confirm accuracy of search criteria, and use reports effectively to demonstrate progress

Approach

Our online instructor-led course provides both live instruction and hands-on exercises to develop the skills needed to successfully implement Spirion.

After your Spirion administrator completes the course, Spirion PS will work with your Spirion administrator to apply their new skills to your environment

Timing

Instructor-Led Training – Our live, remote, instructor-led course takes place over 4 consecutive days. The instruction part of the course can last up to 4 hours, with follow-on assignments for participants to complete in a provided virtual lab environment. The instructor will review exercises with participants at the beginning of each class and be available for assistance after the instructor-led portion to assist with the homework assignments.

Implementation – The implementation phase will begin following the completion of the instructor-led course.

Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion is the leader in data discovery, persistent classification, and protection of sensitive data on-premise and in the cloud. Since 2006, thousands of organizations worldwide have reduced their sensitive data footprint and proactively minimized the risks, costs and reputational damage of successful cyberattacks. Spirion provides greater command and control of sensitive data to leading firms across all industries from financial services to healthcare to public sector. Visit us at spirion.com



ARTICLE 1 – GENERAL

The equipment, materials, or supplies (“Goods”) and/or services (“Services”) furnished by Supplier (together, the “Goods and Services”) and covered by the UC Purchase Order (“PO”) and/or other agreement (which, when combined with these Terms and Conditions and any other documents incorporated by reference, will constitute the “Agreement”) are governed by the terms and conditions set forth herein. As used herein, the term “Supplier” includes Supplier and its sub-suppliers at any tier. As used herein, “UC” refers to The Regents of the University of California, a corporation described in California Constitution Art. IX, Sec. 9, on behalf of the UC Locations identified in the Agreement and/or the PO. UC and Supplier individually will be referred to as “Party” and collectively as “Parties.” Any defined terms not defined in these Terms and Conditions of Purchase will have the meaning ascribed to such term in any of the other documents incorporated in and constituting the Agreement. No other terms or conditions will be binding upon the Parties unless accepted by them in writing. Supplier accepts all of the Agreement’s terms and conditions either in writing, by shipping any portion of the Goods, or performing any portion of the Services. The terms of any proposal referred to in the Agreement are included and made a part of the Agreement only to the extent the proposal specifies the Goods and/or Services ordered, the price therefor, and the delivery thereof, and then only to the extent that such terms are consistent with the terms and conditions of the Agreement.

ARTICLE 2 – TERM AND TERMINATION

- A. As applicable, the term of the Agreement (“Initial Term”) will be stated in the Agreement. Following the Initial Term, the Agreement may be extended by written mutual agreement.
- B. UC’s obligation to proceed is conditioned upon the appropriation of state, federal and other sources of funds not controlled by UC (“Funding”). UC will have the right to terminate the Agreement without damage, penalty, cost or further obligation in the event that through no action or inaction on the part of UC, the Funding is withdrawn.
- C. UC may, by written notice stating the extent and effective date thereof, terminate the Agreement for convenience in whole or in part, at any time. The effective date of such termination shall be consistent with any requirements for providing notice specified in the Agreement, or immediate if no such terms are set forth in the Agreement. As specified in the termination notice, UC will pay Supplier as full compensation the pro rata Agreement price for performance through the later of the date that
 - a. UC provided Supplier with notice of termination or
 - b. Supplier’s provision of Goods and/or Services will terminate.
- D. UC may by written notice terminate the Agreement for Supplier’s breach of the Agreement, in whole or in part, at any time, if Supplier refuses or fails to comply with the provisions of the Agreement, or so fails to make progress as to endanger performance and does not cure such failure within five (5) business days, or fails to supply the Goods and/or Services within the time specified or any written extension thereof. In such event, UC may purchase or otherwise secure Goods and/or Services and, except as otherwise provided herein, Supplier will be liable to UC for any excess costs UC incurs thereby.
- E. If any of the following appendices are incorporated in to the agreement, then they will control in the event that the appendices conflict with the provisions of this Article:
 - UC’s Appendix – Data Security,
 - Appendix – BAA, and/or
 - Appendix – GDPR



Terms and Conditions of Purchase

ARTICLE 3 – PRICING, INVOICING METHOD, AND SETTLEMENT METHOD AND TERMS.

Pricing is set forth in the Agreement or PO, and the amount UC is charged and responsible for shall not exceed the amount specified in the Agreement unless UC has given prior written approval. Unless otherwise agreed in writing by UC, Supplier will use the invoicing method and payment settlement method (and will extend the terms applicable to such settlement method) set forth in UC's Supplier Invoicing, Terms & Settlement Matrix (<https://www.ucop.edu/procurement-services/procurement-systems/supplier-invoicing,-terms-and-settlement-matrix.html>). UC will pay Supplier, upon submission of acceptable invoices, for Goods and/or Services provided and accepted. Invoices must be itemized and reference the Agreement or PO number. UC will not pay shipping, packaging or handling expenses, unless specified in the Agreement or PO. Unless otherwise provided, freight is to be FOB destination. Any of Supplier's expenses that UC agrees to reimburse will be reimbursed under UC's Travel Policy, which may be found at <http://www.ucop.edu/central-travel-management/resources/index.html>. Where applicable, Supplier will pay all taxes imposed on Supplier in connection with its performance under the Agreement, including any federal, state and local income, sales, use, excise and other taxes or assessments. Notwithstanding any other provision to the contrary, UC will not be responsible for any fees, interest or surcharges Supplier wishes to impose.

ARTICLE 4 – INSPECTION.

The Goods and/or Services furnished will be exactly as specified in the Agreement, free from all defects in Supplier's performance, design, skill and materials, and, except as otherwise provided in the Agreement, will be subject to inspection and test by UC at all times and places. If, prior to final acceptance, any Goods and/or Services furnished are found to be incomplete, or not as specified, UC may reject them, require Supplier to correct them at the sole cost of Supplier, or require provision of such Goods and/or Services at a reduction in price that is equitable under the circumstances. If Supplier is unable or refuses to correct such deficiencies within a time UC deems reasonable, UC may terminate the Agreement in whole or in part. Supplier will bear all risks as to rejected Goods and/or Services and, in addition to any costs for which Supplier may become liable to UC under other provisions of the Agreement, will reimburse UC for all transportation costs, other related costs incurred, or payments to Supplier in accordance with the terms of the Agreement for unaccepted Goods and/or Services and materials and supplies incidental thereto. Notwithstanding final acceptance and payment, Supplier will be liable for latent defects, fraud or such gross mistakes as amount to fraud.

ARTICLE 5 – ASSIGNED PERSONNEL; CHARACTER OF SERVICES

Supplier will provide the Services as an independent contractor and furnish all equipment, personnel, and supplies sufficient to provide the Services expeditiously and efficiently, during as many hours per shift and shifts per week, and at such locations as UC may so require. Supplier will devote only its best-qualified personnel to work under the Agreement. Should UC inform Supplier that anyone providing the Services is not working to this standard, Supplier will immediately remove such personnel from providing Services and those individuals will not again be assigned to provide Services without UC's written permission. At no time will Supplier or Supplier's employees, sub-suppliers, agents, or assigns be considered employees of UC for any purpose, including but not limited to workers' compensation provisions. Supplier shall not have the power nor right to bind or obligate UC, and Supplier shall not hold itself out as having such authority. Supplier shall be responsible to UC for all Services performed by Supplier's employees, agents and subcontractors, including being responsible for ensuring payment of all unemployment, social security, payroll, contributions and other taxes with respect to such employees, agents and subcontractors.



ARTICLE 6 – WARRANTIES

In addition to the warranties set forth in Articles 11, 12, 17, 23, 24, 25 and 26 herein, Supplier makes the following warranties. Supplier acknowledges that failure to comply with any of the warranties in the Agreement will constitute a material breach of the Agreement and UC will have the right to terminate the Agreement without damage, penalty, cost or further obligation.

- A. **General Warranties.** Supplier represents, warrants and covenants that: (i) Supplier is free to enter into this Agreement and that Supplier is not, and will not become, during the Term, subject to any restrictions that might restrict or prohibit Supplier from performing the Services or providing the Goods ordered hereunder; (ii) Supplier will comply with all applicable laws, rules and regulations in performing Supplier's obligations hereunder; (iii) the Goods and/or Services shall be rendered with promptness and diligence and shall be executed in a skilled manner by competent personnel, in accordance with the prevailing industry standards; and if UC Appendix Data Security is NOT included: (iv) Supplier has developed a business interruption and disaster recovery program and is executing such program to assess and reduce the extent to which Supplier's hardware, software and embedded systems may be susceptible to errors or failures in various crisis (or force majeure) situations; (v) if Supplier uses electronic systems for creating, modifying, maintaining, archiving, retrieving or transmitting any records, including test results that are required by, or subject to inspection by an applicable regulatory authority, then Supplier represents and warrants that Supplier's systems for electronic records are in compliance; and (vi) Supplier agrees that the Goods and/or Services furnished under the Agreement will be covered by the most favorable warranties Supplier gives to any customer for the same or substantially similar goods or services, or such other more favorable warranties as specified in the Agreement. The rights and remedies so provided are in addition to and do not limit any rights afforded to UC by any other article of the Agreement.
- B. **Permits and Licenses.** Supplier agrees to procure all necessary permits or licenses and abide by all applicable laws, regulations and ordinances of the United States and of the state, territory and political subdivision or any other country in which the Goods and/or Services are provided.
- C. **Federal and State Water and Air Pollution Laws.** Where applicable, Supplier warrants that it complies with the requirements in UC Business and Finance Bulletin BUS-56 (Material Management; Purchases from Entities Violating State or Federal Water or Air Pollution Laws). Consistent with California Government Code 4477, these requirements do not permit UC to contract with entities in violation of Federal or State water or air pollution laws.
- D. **Web Accessibility Requirements.** As applicable to the Supplies and/or Services being provided under the Agreement, Supplier warrants that:
 - a. It complies with California and federal disability laws and regulations; and
 - b. The Goods and/or Services will conform to the accessibility requirements of WCAG 2.0AA.
 - c. Supplier agrees to promptly respond to and resolve any complaint regarding accessibility of its Goods and/or Services;
- E. **General Accessibility Requirements.** Supplier warrants that:
 - a. It will comply with California and federal disability laws and regulations;
 - b. Supplier will promptly respond to remediate to any identified accessibility defects in the Goods and Services to conform to WCAG 2.0 AA; and
 - c. Supplier agrees to promptly respond to and use reasonable efforts to resolve and remediate any complaint regarding accessibility of its Goods and/or Services.
- F. **Warranty of Quiet Enjoyment.** Supplier warrants that Supplier has the right of Quiet Enjoyment in, and conveys the right of Quiet Enjoyment to UC for UC's use of, any and all intellectual property that



UNIVERSITY
OF
CALIFORNIA

Terms and Conditions of Purchase

will be needed for Supplier's provision, and UC's use of, the Goods and/or Services provided by Supplier under the Agreement.

- G. California Child Abuse and Neglect Reporting Act ("CANRA"). Where applicable, Supplier warrants that it complies with CANRA.
- H. Debarment, Suspension, U.S. Government Restricted Party Lists. Supplier warrants that it is not on the U.S. government's Denied Parties List, the Unverified List, the Entities List, the Specially Designated Nationals and Blocked Parties List, and is not presently debarred, suspended, proposed for debarment or otherwise declared ineligible for award of federal contracts or participation in federal assistance programs or activities.
- I. UC Trademark Licensing Code of Conduct. If the Goods will bear UC's name (including UC campus names, abbreviations of these names, UC logos, UC mascots, or UC seals) or other trademarks owned by UC, Supplier warrants that it holds a valid license from UC and complies with the Trademark Licensing Code of Conduct policy, available at <http://policy.ucop.edu/doc/3000130/TrademarkLicensing>
- J. Outsourcing (Public Contract Code section 12147) Compliance. Supplier warrants that if the Agreement will displace UC employees, no funds paid under the Agreement will be used to train workers who are located outside of the United States, or plan to relocate outside the United States as part of the Agreement. Additionally, Supplier warrants that no work will be performed under the Agreement with workers outside the United States, except as described in Supplier's bid. If Supplier or its sub-supplier performs the Agreement with workers outside the United States during the life of the Agreement and Supplier did not describe such work in its bid, Supplier acknowledges and agrees that (i) UC may terminate the Agreement without further obligation for noncompliance, and (ii) Supplier will forfeit to UC the amount UC paid for the percentage of work that was performed with workers outside the United States and not described in Supplier's bid.
- K. Supplier warrants that the Goods and Services rendered under this Agreement will not require Supplier to use for UC, or provide to UC to use, "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system, within the meaning of Federal Acquisition Regulation ("FAR") Section 52.204-25.

Supplier will provide "Timely Notice" to the UC of any changes to the statements, confirmations or representations made in its proposal response or in any information provided as part of the contract award process, including in particular any changes to the certifications or representations made regarding NDAA Section 889. Timely Notice means that Supplier will notify UC in writing within 3 business days of any changes to the representations or confirmations made in relation to NDAA Section 889. Notice shall include the representations or confirmations made and the changes to those representations or confirmations. The notice shall be provided by a Supplier representative authorized to bind the Supplier.

ARTICLE 7 – INTELLECTUAL PROPERTY, COPYRIGHT, PATENTS, AND DATA RIGHTS

- A. Goods and/or Services Involving Work Made for Hire.
 - a. Unless UC indicates that the Goods and/or Services do not involve work made for hire, Supplier acknowledges and agrees that any deliverables provided to UC by Supplier in the performance of the Agreement, and any intellectual property rights therein, (hereinafter the "Deliverables") will be owned by UC. The Deliverables will be considered "work made for hire" under U.S. copyright law and all right, title, and interest to and in such Deliverables including, but not limited to, any and all copyrights or trademarks, will be owned by UC. In



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

the event that it is determined that UC is not the owner of such Deliverables under the "work made for hire" doctrine of U.S. copyright law, Supplier hereby irrevocably assigns to UC all right, title, and interest to and in such Deliverables and any copyrights or trademarks thereto.

- b. The Deliverables must be new and original. Supplier must not use any pre-existing copyrightable or trademarked images, writings, or other proprietary materials (hereinafter "Pre-Existing Materials") in the Deliverables without UC's prior written permission. In the event that Supplier uses any Pre-Existing Materials in the Deliverables in which Supplier has an ownership interest, UC is hereby granted, and will have, a non-exclusive, royalty-free, irrevocable, perpetual, paid-up, worldwide license (with the right to sublicense) to make, have made, copy, modify, make derivative works of, use, perform, display publicly, sell, and otherwise distribute such Pre-Existing Materials in connection with the Deliverables.
 - c. Whenever any invention or discovery is made or conceived by Supplier in the course of or in connection with the Agreement, Supplier will promptly furnish UC with complete information with respect thereto and UC will have the sole power to determine whether and where a patent application will be filed and to determine the disposition of title to and all rights under any application or patent that may result.
 - d. Supplier is specifically subject to an obligation to, and hereby does, assign all right, title and interest in any such intellectual property rights to UC as well as all right, title and interest in tangible research products embodying any such inventions whether the inventions are patentable or not. Supplier agrees to promptly execute any additional documents or forms that UC may require in order to effectuate such assignment.
- B. Goods and/or Services Not Involving Work Made for Hire.**
- a. If the Goods and/or Services do not involve work made for hire, and in the event that Supplier uses any Pre-Existing Materials in the Deliverables in which Supplier has an ownership interest, UC is hereby granted, and will have, a non-exclusive, royalty-free, irrevocable, perpetual, paid-up, worldwide license (with the right to sublicense) to make, have made, copy, modify, make derivative works of, use, perform, display publicly, sell, and otherwise distribute such Pre-Existing Materials in connection with the Deliverables.
 - b. The Deliverables must be new and original. Supplier must not use any Pre-Existing Materials in the Deliverables without UC's prior written permission.
 - c. Whenever any invention or discovery is made or conceived by Supplier in the course of or in connection with the Agreement, Supplier will promptly furnish UC complete information with respect thereto and UC will have the sole power to determine whether and where a patent application will be filed and to determine the disposition of title to and all rights under any application or patent that may result.
 - d. Supplier is specifically subject to an obligation to, and hereby does, assign all right, title and interest in any such intellectual property rights to UC as well as all right, title and interest in tangible research products embodying any such inventions whether the inventions are patentable or not. Supplier agrees to promptly execute any additional documents or forms that UC may require in order to effectuate such assignment.
- C. General.** Should the Goods and/or Services become, or in Supplier's opinion be likely to become, the subject of a claim of infringement of any patent, copyright, trademark, trade name, trade secret, or other proprietary or contractual right of any third party, Supplier will provide written notice to UC of the circumstances giving rise to such claim or likely claim. In the event that UC receives notice of a claim of infringement or is made a party to or is threatened with being made a party to any claim of



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

infringement related to the Goods and/or Services, UC will provide Supplier with notice of such claim or threat. Following receipt of such notice, Supplier will either (at Supplier's sole election) (i) procure for UC the right to continue to use the affected portion of the Goods and/or Services, or (ii) replace or otherwise modify the affected portion of the Goods and/or Services to make them non-infringing, or obtain a reasonable substitute product for the affected portion of the Goods and/or Services, provided that any replacement, modification or substitution under this paragraph does not effect a material change in the Goods and/or Services' functionality. If none of the foregoing options is reasonably acceptable to UC, UC will have the right to terminate the Agreement without damage, penalty, cost or further obligation.

- D. UC Rights to Institutional Information. Institutional Information shall belong exclusively to UC and unless expressly provided, this Agreement shall not be construed as conferring on Supplier any patent, copyright, trademark, license right or trade secret owned or obtained by UC. Any right for Supplier to use Institutional Information is solely provided on a non-exclusive basis, and only to the extent required for Supplier to provide the Goods or Services under the Agreement. As used herein, "Institutional Information" means any information or data created, received, and/or collected by UC or on its behalf, including but not limited to application logs, metadata and data derived from such data.

ARTICLE 8 – INDEMNITY AND LIABILITY

To the fullest extent permitted by law, Supplier will defend, indemnify, and hold harmless UC, its officers, employees, and agents, from and against all losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities of any kind resulting from or arising out of the Agreement, including the performance hereunder of Supplier, its officers, employees, agents, sub-suppliers, or anyone directly or indirectly employed by Supplier, or any person or persons under Supplier's direction and control, provided such losses, expenses, damages and liabilities are due or claimed to be due to the acts or omissions of Supplier, its officers, employees, agents, sub-suppliers, or anyone directly or indirectly employed by Supplier, or any person or persons under Supplier's direction and control. UC agrees to provide Supplier with prompt notice of any such claim or action and to permit Supplier to defend any claim or action, and that UC will cooperate fully in such defense. UC retains the right to participate in the defense against any such claim or action, and the right to consent to any settlement, which consent will not unreasonably be withheld.

In the event Appendix DS applies to this Agreement, Supplier shall reimburse or otherwise be responsible for any costs, fines or penalties imposed against UC as a result of Supplier's Breach of Institutional Information and/or failure to cooperate with UC's response to such Breach. As used herein, "Breach" means:

- a. Any disclosure of Institutional Information to an unauthorized party or in an unlawful manner;
- b. Unauthorized or unlawful acquisition of information that compromises the security, confidentiality or integrity of Institutional Information and/or IT Resources; and
- c. The acquisition, access, use, or disclosure of Protected Health Information or medical information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) or California law. "IT Resources" means IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability that is Supplier owned/managed, or UC-owned, or a personally owned device that stores Institutional Information, is connected to UC systems, is connected to UC networks, or is used for UC business.



ARTICLE 9 – INSURANCE

Supplier, at its sole cost and expense, will insure its activities in connection with providing the Goods and/or Services and obtain, keep in force, and maintain the following insurance with the minimum limits set forth below, unless UC specifies otherwise:

- A. Commercial Form General Liability Insurance (contractual liability included) with limits as follows:
 - a. Each Occurrence \$ 1,000,000
 - b. Products/Completed Operations Aggregate \$ 2,000,000
 - c. Personal and Advertising Injury \$ 1,000,000
 - d. General Aggregate \$ 2,000,000
- B. Business Automobile Liability Insurance for owned, scheduled, non-owned, or hired automobiles with a combined single limit of not less than one million dollars (\$1,000,000) per occurrence. (Required only if Supplier drives on UC premises or transports UC employees, officers, invitees, or agents in the course of supplying the Goods and/or Services to UC.)
- C. If applicable, Professional Liability Insurance with a limit of two million dollars (\$2,000,000) per occurrence or claim with an aggregate of not less than two million dollars (\$2,000,000). If this insurance is written on a claims-made form, it will continue for three years following termination of the Agreement. The insurance will have a retroactive date of placement prior to or coinciding with the effective date of the Agreement.
- D. Workers' Compensation as required by applicable state law and Employer's Liability with limits of one million dollars (\$1,000,000) per occurrence.
- E. If applicable, Supplier Fidelity Bond or Crime coverage for the dishonest acts of its employees in a minimum amount of one million dollars (\$1,000,000). Supplier will endorse such policy to include a "Regents of the University of California Coverage" or "Joint Payee Coverage" endorsement. UC and, if so requested, UC's officers, employees, agents and sub-suppliers will be named as "Loss Payee, as Their Interest May Appear" in such Fidelity Bond.
- F. In the event Appendix DS applies to this Agreement, Supplier, at its sole cost and expense, will obtain, keep in force, and maintain one or more insurance policies that provide coverage for technology, professional liability, data protection, and/or cyber liability. Typically referred to as Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability insurance, it will cover liabilities for financial loss due to the acts, omissions, or intentional misconduct of Supplier, its officers, employees, agents, sub-suppliers, or anyone directly or indirectly employed by Supplier, or any person or persons under Supplier's direction and control, in connection with the performance of this Agreement, as well as all Supplier costs, including damages it is obligated to pay UC or any third party, that are associated with any confirmed or suspected Breach or compromise of Institutional Information. In some cases, Professional Liability policies may include some coverage for data breaches or loss of Institutional Information. Regardless of the type of policy(ies) in place, such coverage will include without limitation:
 - a. Costs to notify parties whose data were lost or compromised;
 - b. Costs to provide credit monitoring and credit restoration services to parties whose data were lost or compromised;
 - c. Costs associated with third party claims arising from the confirmed or suspected Breach or loss of Institutional Information, including litigation costs and settlement costs;
 - d. Any investigation, enforcement, fines and penalties, or similar miscellaneous costs; and
 - e. Any payment made to a third party as a result of extortion related to a confirmed or suspected Breach. The following insurance coverage is based on the highest Protection Level Classification of Institutional Information identified in Exhibit 1 to Appendix DS:



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

- P1 - This insurance policy must have minimum limits of \$500,000 each occurrence and \$500,000 in the aggregate.
- P2 - This insurance policy must have minimum limits of \$1,000,000 each occurrence and \$1,000,000 in the aggregate.
- P3 and P4, less than 70,000 records - this insurance policy must have minimum limits of \$5,000,000 each occurrence and \$5,000,000 in the aggregate.
- P3 and P4, 70,000 or more records - this insurance policy must have minimum limits of \$10,000,000 each occurrence and \$10,000,000 in the aggregate.
- G. Protection Level Classifications are defined in the UC Systemwide Information Security Classification of Information and IT Resources: <https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html>
- H. Additional other insurance in such amounts as may be reasonably required by UC against other insurable risks relating to performance. If the above insurance is written on a claims-made form, it will continue for three years following termination of the Agreement. The insurance will have a retroactive date of placement prior to or coinciding with the effective date of the Agreement. If the above insurance coverage is modified, changed or cancelled, Supplier will provide UC with not less than fifteen (15) days' advance written notice of such modification, change, or cancellation, and will promptly obtain replacement coverage that complies with this Article.
- I. The coverages referred to under A and B of this Article must include UC as an additional insured. It is understood that the coverage and limits referred to under A, B and C of this Article will not in any way limit Supplier's liability. Supplier will furnish UC with certificates of insurance (and the relevant endorsement pages) evidencing compliance with all requirements prior to commencing work under the Agreement. Such certificates will:
- a. Indicate that The Regents of the University of California has been endorsed as an additional insured for the coverage referred to under A and B of this Article. This provision will only apply in proportion to and to the extent of the negligent acts or omissions of Supplier, its officers, agents, or employees.
 - b. Include a provision that the coverage will be primary and will not participate with or be excess over any valid and collectible insurance or program of self-insurance carried or maintained by UC.

ARTICLE 10 – USE OF UC NAME AND TRADEMARKS

Supplier will not use the UC name, abbreviation of the UC name, trade names and/or trademarks (i.e., logos and seals) or any derivation thereof, in any form or manner in advertisements, reports, or other information released to the public, or place the UC name, abbreviations, trade names and/or trademarks or any derivation thereof on any consumer goods, products, or services for sale or distribution to the public, without UC's prior written approval. Supplier agrees to comply at all times with California Education Code Section 92000.

ARTICLE 11 – FEDERAL FUNDS

Supplier who supplies Goods and/or Services certifies and represents its compliance with the following clauses, as applicable. Supplier shall promptly notify UC of any change of status with regard to these certifications and representations. These certifications and representations are material statements upon which UC will rely.



UNIVERSITY
OF
CALIFORNIA

Terms and Conditions of Purchase

- A. For commercial transactions involving funds on a federal contract (federal awards governed by the FAR), the following provisions apply, as applicable:
- a. FAR 52.203-13, Contractor Code of Business Ethics and Conduct;
 - b. FAR 52.203-17, Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights;
 - c. FAR 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements;
 - d. FAR 52.219-8, Utilization of Small Business Concerns;
 - e. FAR 52.222-17, Non-displacement of Qualified Workers;
 - f. FAR 52.222-21, Prohibition of Segregated Facilities;
 - g. FAR 52.222-26, Equal Opportunity;
 - h. FAR 52.222-35, Equal Opportunity for Veterans;
 - i. FAR 52.222-36, Equal Opportunity for Workers with Disabilities;
 - j. FAR 52.222-37, Employment Reports on Veterans;
 - k. FAR 52.222-40, Notification of Employee Rights Under the National Labor Relations Act;
 - l. FAR 52.222-41, Service Contract Labor Standards;
 - m. FAR 52.222-50, Combating Trafficking in Persons;
 - n. FAR 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment - Requirements;
 - o. FAR 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services - Requirements;
 - p. FAR 52.222-54, Employment Eligibility Verification;
 - q. FAR 52.222-55, Minimum Wages Under Executive Order 13658;
 - r. FAR 52.222-62, Paid Sick Leave under Executive Order 13706;
 - s. FAR 52.224-3, Privacy Training;
 - t. FAR 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations;
 - u. FAR 52.233-1, Disputes; and
 - v. FAR 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels.
- B. For non-commercial transactions involving funds on a federal contract, the UC Appendix titled 'Federal Government Contracts Special terms and Conditions (Non-Commercial Items or Services)' and located at www.ucop.edu/procurement-services/policies-forms/index.html is hereby incorporated herein by this reference.
- C. For transactions involving funds on a federal grant or cooperative agreement (federal awards governed by CFR Title 2, Subtitle A, Chapter II, Part 200) the following provisions apply, as applicable:
- a. Rights to Inventions. If Supplier is a small business firm or nonprofit organization, and is providing experimental, development, or research work under this transaction, Supplier must comply with the requirements of 3 CFR Part 401, "Rights to Inventions Made by nonprofit Organizations and Small Business Firms Under Government Grants, Contracts, and Cooperative Agreements".
 - b. Clean Air Act. Supplier agrees 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).
 - c. Byrd Anti-Lobbying. Supplier certifies 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



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

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.

- d. Procurement of Recovered Materials. If Supplier is a state agency or agency of a political subdivision of a state, then Supplier must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act.
 - e. Domestic Preferences for Procurements. As appropriate and to the extent consistent with law, Supplier should, to the greatest extent practicable under a Federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States. "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.
- D. In these provisions, the term "contractor" as used therein will refer to Supplier, and the terms "Government" or "Contracting Officer" as used therein will refer to UC. Where a purchase of items is for fulfillment of a specific U.S. Government prime or subcontract, additional information and/or terms and conditions may be included in an attached supplement. By submitting an invoice to UC, Supplier is representing to UC that, at the time of submission:
- a. Neither Supplier nor its principals are presently debarred, suspended, or proposed for debarment by the U.S. government (see FAR 52.209-6);
 - b. Supplier has filed all compliance reports required by the Equal Opportunity clause (see FAR 52.222-22); and
 - c. Any Supplier representations to UC about U.S. Small Business Administration or state and local classifications, including but not limited to size standards, ownership, and control, are accurate and complete.
 - d. Byrd Anti-Lobbying. Supplier certifies 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.

ARTICLE 12 – EQUAL OPPORTUNITY AFFIRMATIVE ACTION

Supplier will abide by the requirements set forth in Executive Orders 11246 and 11375. Where applicable, Supplier will comply with 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a), incorporated by reference with this statement: "This contractor and subcontractor shall abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status or disability." With respect to activities occurring in the State of California, Supplier agrees to adhere to the California Fair Employment and Housing Act. Supplier will provide UC on request a



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

breakdown of its labor force by groups as specified by UC, and will discuss with UC its policies and practices relating to its affirmative action programs. Supplier will not maintain or provide facilities for employees at any establishment under its control that are segregated on a basis prohibited by federal law. Separate or single-user restrooms and necessary dressing or sleeping areas must be provided, however, to ensure privacy.

ARTICLE 13 – LIENS

Supplier agrees that upon UC's request, Supplier will submit a sworn statement setting forth the work performed or material furnished by sub-suppliers and material men, and the amount due and to become due to each, and that before the final payment called for under the Agreement, will upon UC's request submit to UC a complete set of vouchers showing what payments have been made for such work performed or material furnished. Supplier will promptly notify UC in writing, of any claims, demands, causes of action, liens or suits brought to its attention that arise out of the Agreement. UC will not make final payment until Supplier, if required, delivers to UC a complete release of all liens arising out of the Agreement, or receipts in full in lieu thereof, as UC may require, and if required in either case, an affidavit that as far as it has knowledge or information, the receipts include all the labor and materials for which a lien could be filed; but Supplier may, if any sub-supplier refuses to furnish a release or receipt in full, furnish a bond satisfactory to UC to indemnify it against any claim by lien or otherwise. If any lien or claim remains unsatisfied after all payments are made, Supplier will refund to UC all monies that UC may be compelled to pay in discharging such lien or claim, including all costs and reasonable attorneys' fees.

ARTICLE 14 – PREMISES WHERE SERVICES ARE PROVIDED

- A. Cleaning Up. Supplier will at all times keep UC premises where the Services are performed and adjoining premises free from accumulations of waste material or rubbish caused by its employees or work of any of its sub-suppliers, and, at the completion of the Services; will remove all rubbish from and about the premises and all its tools, scaffolding, and surplus materials, and will leave the premises "broom clean" or its equivalent, unless more exactly specified. In case of dispute between Supplier and its sub-suppliers as to responsibility for the removal of the rubbish, or if it is not promptly removed, UC may remove the rubbish and charge the cost to Supplier.
- B. Environmental, Safety, Health and Fire Protection. Supplier will take all reasonable precautions in providing the Goods and Services to protect the health and safety of UC employees and members of the public and to minimize danger from all hazards to life and property, and will comply with all applicable environmental protection, health, safety, and fire protection regulations and requirements (including reporting requirements). In the event that Supplier fails to comply with such regulations and requirements, UC may, without prejudice to any other legal or contractual rights of UC, issue an order stopping all or any part of the provision of the Goods and/or Services; thereafter a start order for resumption of providing the Goods and/or Services may be issued at UC's discretion. Supplier will not be entitled to make a claim for extension of time or for compensation or damages by reason of or in connection with such stoppage. Supplier will have sole responsibility for the safety of all persons employed by Supplier and its sub-suppliers on UC premises, or any other person who enters upon UC premises for reasons relating to the Agreement. Supplier will at all times maintain good order among its employees and all other persons who come onto UC's premises at Supplier's request and will not engage any unfit or unskilled person to provide the Goods and/or Services. Supplier will confine its employees and all other persons who come onto UC's premises at Supplier's request or for reasons relating to the Agreement and its equipment to



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

that portion of UC's premises where the Services are to be provided or to roads leading to and from such work sites, and to any other area which UC may permit Supplier to use. Supplier will take all reasonable measures and precautions at all times to prevent injuries to or the death of any of its employees or any other person who enters upon UC premises at Supplier's request. Such measures and precautions will include, but will not be limited to, all safeguards and warnings necessary to protect workers and others against any conditions on the premises that could be dangerous and to prevent accidents of any kind whenever the Goods and/or Services are being provided in proximity to any moving or operating machinery, equipment or facilities, whether such machinery, equipment or facilities are the property of or are being operated by, Supplier, its sub-suppliers, UC or other persons. To the extent compliance is required, Supplier will comply with all relevant UC safety rules and regulations when on UC premises.

- C. Tobacco-free Campus. UC is a tobacco-free institution. Use of cigarettes, cigars, oral tobacco, electronic cigarettes and all other tobacco products is prohibited on all UC owned or leased sites.

ARTICLE 15 – LIABILITY FOR UC - FURNISHED PROPERTY

Supplier assumes complete liability for any materials UC furnishes to Supplier in connection with the Agreement and Supplier agrees to pay for any UC materials Supplier damages or otherwise is not able to account for to UC's satisfaction. UC furnishing to Supplier any materials in connection with the Agreement will not, unless otherwise expressly provided in writing by UC, be construed to vest title thereto in Supplier.

ARTICLE 16 – COOPERATION

Supplier and its sub-suppliers, if any, will cooperate with UC and other suppliers and will so provide the Services that other cooperating suppliers will not be hindered, delayed or interfered with in the progress of their work, and so that all of such work will be a finished and complete job of its kind.

ARTICLE 17 – ADDITIONAL TERMS APPLICABLE TO THE FURNISHING OF GOODS

The terms in this Article have special application to the furnishing of Goods:

- A. Price Decreases. Supplier agrees immediately to notify UC of any price decreases from its suppliers, and to pass through to UC any price decreases.
- B. Declared Valuation of Shipments. Except as otherwise provided in the Agreement, all shipments by Supplier under the Agreement for UC's account will be made at the maximum declared value applicable to the lowest transportation rate or classification and the bill of lading will so note.
- C. Title. Title to the Goods purchased under the Agreement will pass directly from Supplier to UC at the f.o.b. point shown, or as otherwise specified in the Agreement, subject to UC's right to reject upon inspection.
- D. Changes. Notwithstanding the terms in Article 34, Amendments, UC may make changes within the general scope of the Agreement in drawings and specifications for specially manufactured Goods, place of delivery, method of shipment or packing of the Agreement by giving notice to Supplier and subsequently confirming such changes in writing. If such changes affect the cost of or the time required for performance of the Agreement, UC and Supplier will agree upon an equitable adjustment in the price and/or delivery terms. Supplier may not make changes without UC's written approval. Any claim of Supplier for an adjustment under the Agreement must be made in writing within thirty (30) days from the date Supplier receives notice of such change unless UC waives this condition in writing. Nothing in the Agreement will excuse Supplier from proceeding with



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

performance of the Agreement as changed hereunder. Supplier may not alter or misbrand, within the meaning of the applicable Federal and State laws, the Goods furnished.

- E. Forced, Convict and Indentured Labor. Supplier warrants that no foreign-made Goods furnished to UC pursuant to the Agreement will be produced in whole or in part by forced labor, convict labor, or indentured labor under penal sanction. If UC determines that Supplier knew or should have known that it was breaching this warranty, UC may, in addition to terminating the Agreement, remove Supplier from consideration for UC contracts for a period not to exceed one year. This warranty is in addition to any applicable warranties in Articles 6 and 11.
- F. Export Control. Supplier agrees to provide UC (the contact listed on the PO) with written notification that identifies the export-controlled Goods and such Goods' export classification if any of the Goods is export-controlled under the International Traffic in Arms Regulations (ITAR) (22 CFR §§ 120-130), the Export Administration Regulations (15 CFR §§ 730-774) 500 or 600 series, or controlled on a military strategic goods list. Supplier agrees to provide UC (the contact listed on the PO) with written notification if Supplier will be providing information necessary for the operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing of the Goods that is beyond a standard user manual (i.e. "Use" technology as defined under the EAR 15 CFR § 772.1), or "Technical Data" (as defined under the ITAR 22 CFR § 120.10).

ARTICLE 18 – CONFLICT OF INTEREST

Supplier affirms that, to the best of Supplier's knowledge, no UC employee who has participated in UC's decision-making concerning the Agreement has an "economic interest" in the Agreement or Supplier. A UC employee's "economic interest" means:

- A. An investment worth \$2,000 or more in Supplier or its affiliate;
- B. A position as director, officer, partner, trustee, employee or manager of Supplier or its affiliate;
- C. Receipt during the past 12 months of \$500 in income or \$440 in gifts from Supplier or its affiliate; or
- D. A personal financial benefit from the Agreement in the amount of \$250 or more.

In the event of a change in these economic interests, Supplier will provide written notice to UC within thirty (30) days after such change, noting such changes. Supplier will not be in a reporting relationship to a UC employee who is a near relative, nor will a near relative be in a decision making position with respect to Supplier.

ARTICLE 19 – AUDIT REQUIREMENTS

The Agreement, and any pertinent records involving transactions relating to this Agreement, is subject to the examination and audit of the Auditor General of the State of California or Comptroller General of the United States or designated Federal authority for a period of up to five (5) years after final payment under the Agreement. UC, and if the underlying grant, cooperative agreement or federal contract so provides, the other contracting Party or grantor (and if that be the United States or an instrumentality thereof, then the Comptroller General of the United States) will have access to and the right to examine Supplier's pertinent books, documents, papers, and records involving transactions and work related to the Agreement until the expiration of five (5) years after final payment under the Agreement. The examination and audit will be confined to those matters connected with the performance of the Agreement, including the costs of administering the Agreement.

ARTICLE 20 – PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF INSTITUTIONAL INFORMATION



Terms and Conditions of Purchase

- A. Prohibition on Access, Use and Disclosure of Institutional Information. Supplier will not access, use or disclose Institutional Information, other than to carry out the purposes for which UC disclosed the Institutional Information to Supplier, except as required by applicable law, or as otherwise authorized in writing by UC prior to Supplier's disclosure. Supplier shall have the limited right to disclose Institutional Information to Supplier's employees provided that: (i) Supplier shall disclose only such Institutional Information as is necessary for the Supplier to perform its obligations under this Agreement, and (ii) Supplier informs such employees of the obligations governing the access, use and disclosure of Institutional Information prior to Supplier's disclosure. Supplier shall be liable for any breach of this Agreement by its employees. For avoidance of doubt, this provision prohibits Supplier from using for its own benefit Institutional Information and any information derived therefrom. For the avoidance of doubt, the sale of Institutional Information is expressly prohibited.
- B. Compliance with Applicable Laws and Industry Best Practices. Supplier agrees to comply with all applicable state, federal, and foreign laws, as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Institutional Information. Supplier agrees to protect the privacy and security of Institutional Information according to all applicable laws and industry best practices, and no less rigorously than it protects its own information, but in no case less than reasonable care.
- C. Confidential Institutional Information. Supplier agrees to hold UC's Confidential Institutional Information, and any information derived therefrom, in strict confidence. Confidential Institutional Information shall be defined as any Institutional Information which is (i) marked as "Confidential" at the time of disclosure; (ii) if disclosed orally, identified at the time of such oral disclosure as confidential, and reduced to writing as "Confidential" within thirty (30) days of such oral disclosure; and (iii) if not marked as "Confidential," information that would be considered by a reasonable person in the relevant field to be confidential given its content and the circumstances of its disclosure. Confidential Information will not be considered confidential to the extent that: (i) Supplier can demonstrate by written records was known to Supplier prior to the effective date of the Agreement; (ii) is currently in, or in the future enters, the public domain other than through a breach of the Agreement or through other acts or omissions of Supplier; (iii) is obtained lawfully from a third party; or (iv) is disclosed under the California Public Records Act or legal process. For the avoidance of doubt, as applicable to Supplier's Services, Confidential Institutional Information may include any information that identifies or is capable of identifying a specific individual, including but not limited to:
- a. Personally identifiable information,
 - b. Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA regulations (including, but not limited to 45 C.F.R. § 160.103),
 - c. Medical information as defined by California Civil Code § 56.05,
 - d. Cardholder data,
 - e. Student records, or
 - f. Individual financial information that is subject to laws restricting the use and disclosure of such information, including but not limited to:
 - i. Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 et seq.);
 - ii. The federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2));
 - iii. The federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g);
 - iv. The federal Fair and Accurate Credit Transactions Act (15 U.S.C. § 1601 et seq.);



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

- v. The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq), and
 - vi. Applicable international privacy laws, including, but not limited to the General Data Protection Regulation.
- D. Required Disclosures of Institutional Information. If Supplier is required by a court of competent jurisdiction or an administrative body to disclose Institutional Information, Supplier will notify UC in writing immediately upon receiving notice of such requirement and prior to any such disclosure (unless Supplier is prohibited by law from doing so), to give UC an opportunity to oppose or otherwise respond to such disclosure. To the extent Supplier still required to disclose Institutional Information, Supplier will furnish only that portion that is legally required and will exercise all reasonable efforts to obtain reliable assurance that confidential treatment will be afforded to any Confidential Institutional Information.
- E. No Offshoring. Supplier's transmission, transportation or storage of Institutional Information outside the United States, or access of Institutional Information from outside the United States, is prohibited except with prior written authorization by UC.
- F. Conflict in Terms. UC's Appendix – Data Security, Appendix – BAA, and/or Appendix GDPR will control in the event that one or more appendices is incorporated into the Agreement and conflicts with the provisions of this Article.
- G. Acknowledgement. Supplier acknowledges that remedies at law would be inadequate to protect UC against any actual or threatened breach of this Section by Supplier, and, without prejudice to any other rights and remedies otherwise available to UC, Supplier agrees to the granting of injunctive relief in UC's favor without proof of actual damages.

ARTICLE 21 – UC WHISTLEBLOWER POLICY

UC is committed to conducting its affairs in compliance with the law, and has established a process for reporting and investigating suspected improper governmental activities. Please visit <http://www.ucop.edu/uc-whistleblower/> for more information.

ARTICLE 22 – SUSTAINABLE PROCUREMENT GUIDELINES

Supplier will conduct business using environmentally, socially, and economically sustainable products and services (defined as products and services with a lesser or reduced effect on human health and the environment, and which generate benefits to the University as well as to society and the economy, while remaining within the carrying capacity of the environment), to the maximum possible extent consistent with the Agreement, and with the University of California Sustainable Practices Policy (<https://policy.ucop.edu/doc/3100155>) and the University of California Sustainable Procurement Guidelines:

<https://www.ucop.edu/procurement-services/for-ucstaff/sustainable-procurement/sustainableprocurementguidelines.pdf>

In accordance with the University of California Sustainable Practices Policy, Supplier will adhere to the following requirements and standards, as applicable. Supplier acknowledges that failure to comply with any of the sustainability standards and requirements in the Agreement will constitute a material breach of the Agreement and UC will have the right to terminate the Agreement without damage, penalty, cost or further obligation.

- A. Sustainability Marketing Standards. Supplier sustainability related claims, where applicable, must meet UC recognized certifications and standards set forth in the UC Sustainable Procurement Guidelines and/or meet the standards of Federal Trade Commission's (FTC) Green Guides.



Terms and Conditions of Purchase

- B. Electronic Transfer of Supplier Information. Suppliers, when interacting with the UC, shall be prohibited from providing hard copies of presentations, marketing material, or other informational materials. Suppliers will be required to present all information in electronic format that is easily transferable to UC staff. Materials may be provided in hard copy or physical format if specifically required or requested by a UC representative.
- C. Packaging Requirements. All packaging must be compliant with the Toxics in Packaging Prevention Act (AB 455) and must meet all additional standards and requirements set forth in the UC Sustainable Practices Policy. In addition, UC requires that all packaging meet at least one of the criteria listed below:
- a. Uses bulk packaging;
 - b. Uses reusable packaging (e.g. totes reused by delivery service for next delivery);
 - c. Uses innovative packaging that reduces the weight of packaging, reduces packaging waste, or utilizes packaging that is a component of the product;
 - d. Maximizes recycled content and/or meets or exceeds the minimum post-consumer content level for packaging in the U.S. Environmental Protection Agency Comprehensive Procurement Guidelines;
 - e. Uses locally recyclable or certified compostable material.
- D. Foodservice Foam Ban. As of 2018, the University no longer allows packaging foam or expanded polystyrene (EPS) for takeaway containers or other food service items, in any University-owned or -operated food service facility.
- E. Product Packaging Foam Ban. Beginning January 1st, 2020, the University will prohibit all contracted and non-contracted suppliers from selling or distributing packaging foam (other than that utilized for laboratory supply or medical packaging) to UC campuses. Packaging foam is defined as any open or closed cell, solidified, polymeric foam used for cushioning or packaging, including but not limited to: low-density polyethylene foam, polypropylene foam, polystyrene foam (i.e. expanded polystyrene (EPS)), polyurethane foam, polyethylene foam, polyvinyl chloride (PVC) foam, and microcellular foam. Not included in this ban are easily biodegradable, plant-based foams such as those derived from corn or mushrooms.
- F. E-Waste Recycling Requirements. All recyclers of UC electronic equipment must be e-Steward certified by the Basel Action Network (BAN).
- G. Hosted and Punch-out Catalog Requirements. Suppliers enabled with eProcurement hosted catalog functionality must clearly identify products with UC-recognized certifications, as defined by the UC Sustainable Procurement Guidelines, in both hosted and punch-out catalog e-procurement environments.

ARTICLE 23 – PATIENT PROTECTION AND AFFORDABLE CARE ACT (PPACA) EMPLOYER SHARED RESPONSIBILITY

If the Services involve Supplier furnishing UC with temporary or supplementary staffing, Supplier warrants that:

- A. If Supplier is an Applicable Large Employer (as defined under Treasury Regulation Section 54.4980H-1(a)(4)):
- a. Supplier offers health coverage to its full-time employees who are performing Services for UC;
 - b. Supplier's cost of enrolling such employees in Supplier's health plan is factored into the fees for the Services; and



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

- c. The fees for the Services are higher than what the Services would cost if Supplier did not offer health coverage to such full-time employees.
- B. If Supplier is not an Applicable Large Employer (as defined above):
 - a. Supplier offers group health coverage to its full-time employees who are performing Services for UC and such coverage is considered Minimum Essential Coverage (as defined under Treasury Regulation Section 1-5000A-2) and is Affordable (as defined under Treasury Regulation Section 54.4980H-5(e)); or
 - b. Supplier's full-time employees who are performing services for UC have individual coverage and such coverage satisfies the PPACA requirements for mandated individual coverage.
- C. Supplier acknowledges that UC is relying on these warranties to ensure UC's compliance with the PPACA Employer Shared Responsibility provision.

ARTICLE 24 - PREVAILING WAGES

Unless UC notifies Supplier that the Services are not subject to prevailing wage requirements, Supplier will comply, and will ensure that all sub-suppliers comply, with California prevailing wage provisions, including but not limited to those set forth in Labor Code sections 1770, 1771, 1771.1, 1772, 1773, 1773.1, 1774, 1775, 1776, 1777.5, and 1777.6. For purposes of the Agreement, the term "sub-supplier" means a person or firm, of all tiers, that has a contract with Supplier or with a sub-supplier to provide a portion of the Services. The term sub-supplier will not include suppliers, manufacturers, or distributors. Specifically, and not by way of limitation, if apprenticeship occupations are involved in providing the Services, Supplier will be responsible for ensuring that Supplier and any sub-suppliers comply with Labor Code Section 1777.5. Supplier and sub-supplier may not provide the Services unless currently registered and qualified to perform public work pursuant to Labor Code Section 1725.5 and 1771.1.

Notwithstanding the foregoing provisions, Supplier will be solely responsible for tracking and ensuring proper payment of prevailing wages regardless if Services are partially or wholly subject to prevailing wage requirements. In every instance, Supplier will pay not less than the UC Fair Wage (defined as \$13 per hour as of 10/1/15, \$14 per hour as of 10/1/16, and \$15 per hour as of 10/1/17) for Services being performed at a UC Location (defined as any location owned or leased by UC).

The California Department of Industrial Relations (DIR) has ascertained the general prevailing per diem wage rates in the locality in which the Services are to be provided for each craft, classification, or type of worker required to provide the Services. A copy of the general prevailing per diem wage rates will be on file at each UC Location's procurement office, and will be made available to any interested party upon request. Supplier will post at any job site:

- A. Notice of the general prevailing per diem wage rates, and
- B. Any other notices required by DIR rule or regulation

By this reference, such notices are made part of the Agreement. Supplier will pay not less than the prevailing wage rates, as specified in the schedule and any amendments thereto, to all workers employed by Supplier in providing the Services. Supplier will cause all subcontracts to include the provision that all sub-suppliers will pay not less than the prevailing rates to all workers employed by such sub-suppliers in providing the Services. The Services are subject to compliance monitoring and enforcement by the DIR. Supplier will forfeit, as a penalty, not more than \$200 for each calendar day or portion thereof for each worker that is paid less than the prevailing rates as determined by the DIR for the work or craft in which the worker is employed for any portion of the Services provided by Supplier or any sub-supplier. The amount of this penalty will be determined pursuant to applicable law. Such



UNIVERSITY
OF
CALIFORNIA

Terms and Conditions of Purchase

forfeiture amounts may be deducted from the amounts due under the Agreement. If there are insufficient funds remaining in the amounts due under the Agreement, Supplier will be liable for any outstanding amount remaining due. Supplier will also pay to any worker who was paid less than the prevailing wage rate for the work or craft for which the worker was employed for any portion of the Services, for each day, or portion thereof, for which the worker was paid less than the specified prevailing per diem wage rate, an amount equal to the difference between the specified prevailing per diem wage rate and the amount which was paid to the worker. Review of any civil wage and penalty assessment will be made pursuant to California Labor Code section 1742.

ARTICLE 25 – FAIR WAGE/FAIR WORK

If the Agreement is for Services that will be performed at one or more UC Locations, does not solely involve furnishing Goods, and are not subject to extramural awards containing sponsor-mandated terms and conditions, Supplier warrants that it is in compliance with applicable federal, state and local working conditions requirements, including but not limited to those set forth in Articles 11, 12 and 14 herein, and that Supplier pays its employees performing the Services no less than the UC Fair Wage. Supplier agrees UC may conduct such UC Fair Wage/Fair Work interim compliance audits as UC reasonably requests, as determined in UC's sole discretion. Supplier agrees to post UC Fair Wage/Fair Work notices, in the form supplied by UC, in public areas (such as break rooms and lunch rooms) frequented by Supplier employees who perform Services.

For Services rendered (actual spend) not subject to prevailing wage requirements in excess of \$100,000 in a year (under the Agreement or any combination of agreements for the same service), Supplier will

- a. At Supplier's expense, provide an annual independent verification (<https://www.ucop.edu/procurement-services/for-suppliers/fww-resources-suppliers.html>) performed by a licensed public accounting firm (independent accountant) or the Supplier's independent internal audit department (<http://na.theiia.org/standards-guidance/topics/Pages/Independence-and-Objectivity.aspx>) in compliance with UC's required verification standards and procedures (<https://www.ucop.edu/procurement-services/for-suppliers/fww-resources-suppliers.html>), concerning Supplier's compliance with this provision, and
- b. Ensure that in the case of a UC interim audit, its independent accountant/independent internal auditor makes available to UC its work papers for UC Fair Wage/Fair Work for the most recent verification period. Supplier agrees to provide UC with a UC Fair Wage/Fair Work verification annually, in a form acceptable to UC, no later than ninety days after the end of the 12-month period in which \$100,000 in spend is reached.

The Fair Wage Fair Work annual independent verification requirement does not extend to contracts for professional services or consulting for which pre-certification has been provided to UC (<https://www.ucop.edu/procurement-services/for-suppliers/fww-resources-suppliers.html>). Please see the UC Procurement/Supply Chain Management Policy BUS-43 (<https://www.ucop.edu/procurement-services/policies-forms/business-and-finance/index.html>) for the definition of professional services and consulting.

ARTICLE 26 – MEDICAL DEVICES



UNIVERSITY
OF
CALIFORNIA

Terms and Conditions of Purchase

This Article applies when the Goods and/or Services involve UC purchasing or leasing one or more medical devices from Supplier, or when Supplier uses one or more medical devices in providing Goods and/or Services to UC.

Medical Device as used herein will have the meaning provided by the U.S. Food and Drug Administration ("FDA") and means an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

- a. Recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them;
- b. Intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in humans or other animals, or
- c. Intended to affect the structure or any function of the body of humans or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of humans or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes.

Supplier warrants that prior to UC's purchase or lease of any Medical Device or Supplier's use of any Medical Device in providing Goods and/or Services hereunder, Supplier will:

- a. Perform security testing and validation for each such Goods and/or Services or Medical Device, as applicable;
- b. Perform security scans to detect malware on any software embedded within any Goods and/or Services or Medical Device, as applicable, in order to verify that the software does not contain any known malware;
- c. Conduct a vulnerability scan encompassing all ports and fuzz testing; and
- d. Provide UC with reports for a-c. Supplier warrants that all Goods or Medical Devices are compliant with FDA's most current guidance or regulation for the quality system related to the cybersecurity and the Management of Cybersecurity in Medical Devices, and that Supplier will maintain compliance with any updates to such guidance or regulations.

Throughout Supplier's performance of this Agreement, Supplier will provide UC with reasonably up-to-date patches, firmware and security updates for any Medical Device provided to UC, and any other Medical Device used in the course of providing Services, as applicable. All such patches and other security updates will be made available to UC within thirty (30) days of its commercial release or as otherwise recommended by Supplier or Supplier's sub-supplier, whichever is earlier.

Supplier warrants that all software and installation media not specifically required for any Medical Device used by Supplier or Goods and/or Services delivered to UC under this Agreement as well as files, scripts, messaging services and data will be removed from all such Goods and/or Services or Medical Device following installation, and that all hardware ports and drivers not required for use or operation of such Goods and/or Services or Medical Device will be disabled at time of installation. In addition, Medical Devices must be configured so that only Supplier-approved applications will run on such Medical Devices.

Supplier agrees that UC may take any and all actions that it, in its sole discretion, deems necessary to address, mitigate and/or rectify any real or potential security threat, and that no such action, to the



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

extent such action does not compromise device certification, will impact, limit, reduce or negate Supplier's warranties or any of Supplier's other obligations hereunder.

Supplier warrants that any Medical Device provided to UC, and any other Medical Device used in the course of providing such Goods and/or Services, meet and comply with all cyber-security guidance and similar standards promulgated by the FDA and any other applicable regulatory body.

If the Goods and/or Services entail provision or use of a Medical Device, Supplier will provide UC with a completed Manufacturer Disclosure Statement for Medical Device Security (MDS2) form for each such Medical Device before UC is obligated to purchase or lease such Medical Device or prior to Supplier's use of such device in its performance of Services. If Supplier provides an MDS2 form to UC concurrently with its provision of Goods and/or Services, UC will have a reasonable period of time to review such MDS2 form, and if the MDS2 form is unacceptable to UC, then UC in its sole discretion may return the Goods or terminate the Agreement with no further obligation to Supplier.

ARTICLE 27 – FORCE MAJEURE

Neither Party shall be deemed to be in default of or to have breached any provision of this Agreement due to a delay, failure in performance or interruption of service, if such performance or service are impossible to execute, illegal or commercially impracticable, because of the following "force majeure" occurrences: acts of God, acts of civil or military authorities, civil disturbances, wars, strikes or other labor disputes, transportation contingencies, freight embargoes, acts or orders of any government or agency or official thereof, earthquakes, fires, floods, unusually severe weather, epidemics, pandemics, quarantine restrictions and other catastrophes or any other similar occurrences beyond such party's reasonable control. In every case, the delay or failure in performance or interruption of service must be without the fault or negligence of the Party claiming excusable delay and the Party claiming excusable delay must promptly notify the other Party of such delay. Performance time under this Agreement shall be considered extended for a period of time equivalent to the time lost because of the force majeure occurrence; provided, however, that if any such delay continues for a period of more than thirty (30) days, UC shall have the option of terminating this Agreement upon written notice to Supplier.

ARTICLE 28 – ASSIGNMENT AND SUBCONTRACTING

Except as to any payment due hereunder, Supplier may not assign or subcontract the Agreement without UC's written consent. In case such consent is given, the assignee or subcontractor will be subject to all of the terms of the Agreement.

ARTICLE 29 – NO THIRD-PARTY RIGHTS

Nothing in the Agreement, express or implied, is intended to make any person or entity that is not a signer to the Agreement a third-party beneficiary of any right created by this Agreement or by operation of law.

ARTICLE 30 – OTHER APPLICABLE LAWS

Any provision required to be included in a contract of this type by any applicable and valid federal, state or local law, ordinance, rule or regulations will be deemed to be incorporated herein.

ARTICLE 31 – NOTICES



**UNIVERSITY
OF
CALIFORNIA**

Terms and Conditions of Purchase

A Party must send any notice required to be given under the Agreement by overnight delivery or by certified mail with return receipt requested, to the other Party's representative at the address specified by such Party.

ARTICLE 32 – SEVERABILITY

If a provision of the Agreement becomes, or is determined to be, illegal, invalid, or unenforceable, that will not affect the legality, validity or enforceability of any other provision of the Agreement or of any portion of the invalidated provision that remains legal, valid, or enforceable.

ARTICLE 33 – WAIVER

Waiver or non-enforcement by either Party of a provision of the Agreement will not constitute a waiver or non-enforcement of any other provision or of any subsequent breach of the same or similar provision.

ARTICLE 34 – AMENDMENTS

The Parties may make changes in the Goods and/or Services or otherwise amend the Agreement, but only by a writing signed by both Parties' authorized representatives. In the event there is a Material Change to the Agreement, the parties agree to meet and confer in good faith in order to modify the terms of the Agreement. A Material Change as used herein refers to:

- a. A change to the scope of Goods and/or Services to be provided by Supplier, as agreed to by UC;
- b. A change in the Institutional Information Supplier is required to create, receive, maintain or transmit in performance of the Agreement, such that the Protection Level Classification of such Institutional Information changes;
- c. Changes in the status of the parties;
- d. Changes in flow down terms from external parties; and
- e. Changes in law or regulation applicable to this Agreement.

Each party shall notify the other party upon the occurrence of a Material Change.

ARTICLE 35 – GOVERNING LAW AND VENUE

California law will control the Agreement and any document to which it is appended. The exclusive jurisdiction and venue for any and all actions arising out of or brought under the Agreement is in a state court of competent jurisdiction, situated in the county in the State of California in which the UC Location is located or, where the procurement covers more than one UC Location, the exclusive venue is Alameda County, California.

ARTICLE 36 – ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

Supplier will make itself and its employees, subcontractors, or agents assisting Supplier in the performance of its obligations reasonably available to UC at no cost to UC to testify as witnesses, or otherwise, in the event of investigations, or proceedings against UC, its directors, officers, agents, or employees relating to the Goods or Services.

ARTICLE 37 – SUPPLIER TERMS

Any additional terms that Supplier includes in an order form or similar document will be of no force and effect, unless UC expressly agrees in writing to such terms.



Terms and Conditions of Purchase

ARTICLE 38 – SURVIVAL CLAUSE

Upon expiration or termination of the Agreement, the following provisions will survive: WARRANTIES; INTELLECTUAL PROPERTY, COPYRIGHT, PATENTS, AND DATA RIGHTS; INDEMNITY AND LIABILITY; USE OF UC NAMES AND TRADEMARKS; LIABILITY FOR UC-FURNISHED PROPERTY; COOPERATION; TERMS APPLICABLE TO THE FURNISHING OF GOODS; AUDIT REQUIREMENTS; PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF INSTITUTIONAL INFORMATION; GOVERNING LAW AND VENUE, and, to the extent incorporated into the Agreement, the terms of the APPENDIX–DATA SECURITY, APPENDIX–BAA, and/or APPENDIX–GDPR.

ARTICLE 39 – CONTRACTING FOR COVERED SERVICES

Covered Services, for the purpose of this Agreement, are defined as work customarily performed by bargaining unit employees at the University in the categories of services described in Regents Policy 5402, and American Federation of State, County, and Municipal Employees (AFSCME) Collective Bargaining Agreement Article 5. Covered Services include, but are not necessarily limited to, the following services: cleaning, custodial, janitorial, or housekeeping services; food services; laundry services; grounds keeping; building maintenance (excluding skilled crafts); transportation and parking services; security services; billing and coding services; sterile processing; hospital or nursing assistant services; and medical imaging or other medical technician services.

Unless UC notifies Supplier that the Services are not Covered Services, Supplier warrants that it is in compliance with applicable federal, state and local working conditions requirements, including but not limited to those set forth in in other Articles of the Agreement. In accordance with Regents Policy 5402 and AFSCME Collective Bargaining Agreement Article 5, Supplier also warrants that it pays its employees performing the Covered Services at UC locations the equivalent value of the wages and benefits – as determined in the Wage and Benefit Parity Appendix – received by UC employees providing similar services at the same, or nearest UC location.

Supplier agrees UC may conduct such compliance audits as UC reasonably requests, and determined at UC's sole discretion. Supplier agrees to post UC Contracting for Covered Services notices, in the template supplied by UC, in a prominent and accessible place (such as break rooms and lunch rooms) where it may be easily seen by workers who perform Covered Services. The term "Supplier" includes Supplier and its Sub-Suppliers at any tier. Supplier also agrees to:

- a. Upon UC's request, provide verification of an independent audit performed by Supplier's independent auditor or independent internal audit department (<http://na.theiia.org/standards-guidance/topics/Pages/Independence-and-Objectivity.aspx>) and at Supplier's expense; and
- b. Ensure that, in the case of a UC interim audit, Supplier's auditor makes available to UC its Contracting for Covered Services work papers for the most recently audited time period. Supplier agrees to provide UC requested verification, in a form acceptable to UC, no later than ninety days after receiving UC's request.

**ARTICLE 1. PURPOSE AND INTRODUCTION**

- A. In the course of providing the Goods and/or Services contemplated by the Agreement, Supplier may gain access to the University of California's (UC) Institutional Information and/or IT Resources (both defined below). In such an event, UC and Supplier desire to appropriately protect Institutional Information and IT Resources. The purpose of this Appendix-Data Security is to specify Supplier's cybersecurity and risk management responsibilities when Supplier has access to Institutional Information and/or IT Resources.
- B. Any capitalized terms used here have the meaning ascribed to such terms as set forth in the Agreement or Incorporated Documents.
- C. Supplier must provide commercially acceptable cybersecurity and cyber risk management to protect Institutional Information and/or IT Resources. This must include, but is not limited to the Supplier:
1. Developing and documenting a plan that protects Institutional Information and IT Resources.
 - Supplier must responsibly execute this plan.
 - Supplier's approach must conform to a recognized cybersecurity framework designed for that purpose.¹
 - Supplier's information security plan must be supported by a third-party review or certification. Supplier may only use an alternative to a third-party review if approved by the responsible UC Information Security Officer.
 2. Conducting an accurate and thorough assessment of the potential risks to and vulnerabilities of the security of the Institutional Information and/or IT Resources. Supplier must mitigate anticipated risks effectively. This includes implementing commercially acceptable security policies, procedures, and practices that protect Institutional Information and/or IT Resources.
 3. Updating its plan to effectively address new cybersecurity risks.
 4. Complying with pertinent contractual and regulatory responsibilities.
 5. Providing UC with evidence of compliance with Supplier's information security plan.
 6. Keeping UC informed with timely updates on risks, vulnerabilities, Security Incidents, and Breaches.
 7. Keeping UC informed of any measures UC must perform to ensure the security of Institutional Information and IT Resources.

¹ Examples include the latest versions of PCI DSS, NIST CSF, CIS Critical Security Controls, ISO 27002, NIST SP 800-53 and NIST SP 800-171.

- D. If, in the course of providing the Goods and/or Services under the Agreement, Supplier engages in transactions with UC affiliated individuals (including but not limited to: students, staff, faculty, customers, patients, guests, volunteers, visitors, research subjects, etc.), as a benefit and result of the Agreement, Supplier must treat any data about UC affiliated individuals that Supplier creates, receives, and/or collects in the course of those transactions with the same level of privacy and security protections and standards as required of Institutional Information by this Appendix.
- E. Supplier agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Supplier also agrees to impose, by written contract, the same terms and conditions contained in this Appendix on any sub-supplier retained by Supplier to provide or assist in providing the Goods and/or Services to UC.
- F. To the extent that a requirement of this Appendix conflicts with those of any other UC Agreement or Incorporated Document, the most stringent requirement (including but not limited to: least risk to UC, shortest time, best practice, etc.) will apply.

ARTICLE 2. DEFINED TERMS

- A. **“Breach”** means: (1) Any disclosure of Institutional Information to an unauthorized party or in an unlawful manner; (2) Unauthorized or unlawful acquisition of information that compromises the security, confidentiality, or integrity of Institutional Information and/or IT Resources; or (3) The acquisition, access, use, or disclosure of protected health information (PHI) or medical information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) or California law.
- B. **“Illicit Code”** means: (1) Any code UC would not reasonably expect to be present or operating; (2) Hidden software or functionality with adverse or undesired actions or consequences; (3) Code that replicates or transmits Institutional Information or activates operating systems or other similar services without the express knowledge and approval of UC; (4) Code that alters, damages, or erases any Institutional Information or software without the express knowledge and approval of UC; or (5) Code or apparatus that functions in any way as a: key lock, node lock, time-out, “back door,” “trap door,” “booby trap,” “dead drop device,” “data scrambling device,” or other function, regardless of how it is implemented, which is intended to alter or restrict the use of or access to any Institutional Information and/or IT Resources.
- C. **“Institutional Information”** means: Any information or data created, received, and/or collected by UC or on its behalf, including but not limited to: application logs, metadata, and data derived from such data.
- D. **“IT Resource”** means: IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability that is Supplier owned/managed or UC-owned, or a personally owned device that stores Institutional Information, is connected to UC systems, is connected to UC networks, or is used for UC business. IT Resources include, but are not limited to: personal and mobile computing systems and devices,

mobile phones, printers, network devices, industrial control systems (including but not limited to: SCADA, PLCs, DPC, Operational Technology, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens, Internet of Things (IoT), or any other device that connects to any UC network.

E. **“Major Change”** means: The implementation of a change that could have an effect on the security of an IT Resource or Institutional Information. The scope includes changes to architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items. These include changes related to:

1. Technology upgrades or migrations.
2. Responses to Security Incidents.
3. Modifications of scope (data elements, features, location of Institutional Information, etc.).
4. Regulatory guidance.
5. Law and legal regulations.
6. Responses to risk assessments.
7. Addressing vulnerabilities.
8. Material updates or shifts in technologies used by Supplier.

F. **“Security Incident”** means: (1) A material compromise of the confidentiality, integrity, or availability of Institutional Information; (2) A single event or a series of unwanted or unexpected events that has a significant probability of compromising UC business operations or threatening Institutional Information and/or IT Resources; (3) Any event involving a cyber intrusion; or (4) A material failure of Supplier’s administrative, technical, or physical controls that resulted or could have resulted in an adverse impact to the confidentiality, integrity, or availability of Institutional Information or IT Resources.

ARTICLE 3. ACCESS TO INSTITUTIONAL INFORMATION AND IT RESOURCES

A. Supplier must limit its access to, use of, and disclosure of Institutional Information and IT Resources to the least invasive degree necessary required to provide the Goods and/or Services.

1. Supplier may not access or use Institutional Information and IT Resources for any purpose except to provide the Goods and/or Services.
2. For the avoidance of doubt, Supplier may not access, use, or disclose Institutional Information and IT Resources outside the scope of the Agreement for purposes of, including but not limited to: marketing, advertising, research, sale, or licensing unless expressly approved in writing by UC.

B. In the event that Goods and/or Services include the review of a specific Security Incident or a threat to or anomaly in Institutional Information or IT Resources, Supplier must limit inspection to the least invasive degree necessary required to perform the investigation.

ARTICLE 4. SUPPLIER'S INFORMATION SECURITY PLAN AND RESPONSIBILITIES

- A. Supplier acknowledges that UC must comply with information security standards as required by law, regulation, and regulatory guidance, as well as by UC's internal security program that protects Institutional Information and IT Resources.
- B. Supplier must establish, maintain, comply with, and responsibly execute its information security plan.
- C. Supplier's initial information security plan is attached as Exhibit 2 and incorporated by reference.
- D. Updates to Exhibit 2 will occur as follows:
1. On an annual basis, Supplier will review its information security plan, update it as needed, and submit it upon written request by UC.
 2. In the event of a Major Change, Supplier will review its information security plan, update it as needed, and submit it to UC as detailed herein.
- E. If Supplier makes any material modifications to its information security plan that will affect the security of Institutional Information and IT Resources, Supplier must notify UC within seventy-two (72) calendar hours and identify the changes.
- F. Supplier's Information Security Plan must:
1. Ensure the security (including but not limited to: confidentiality, integrity, and availability) of Institutional Information and IT Resources through the use and maintenance of appropriate administrative, technical, and physical controls;
 2. Protect against any reasonably anticipated threats or hazards to Institutional Information and IT Resources;
 3. Address the risks associated with Supplier having access to Institutional Information and IT Resources;
 4. Comply with applicable regulations and/or external obligations listed in Exhibit 1;
 5. Comply with all applicable legal and regulatory requirements for data protection, security, and privacy;
 6. Clearly document the cybersecurity responsibilities of each party;
 7. Follow UC records retention requirements outlined in the Statement of Work (SOW) or in UC's Terms and Conditions;
 8. Prevent the sharing of passwords or authentication secrets that provide access to Institutional Information and/or IT Resources;
 9. Prevent the use of passphrases (passwords) or other authentication secrets that are common across customers or multiple unrelated UC sites or units;
 10. Prevent unauthorized access to Institutional Information and IT Resources;
 11. Prevent unauthorized changes to IT Resources;
 12. Prevent the reduction, removal, or turning off of any security control without express written approval from UC;

13. Prevent the creation of new Supplier accounts to access Institutional Information and IT Resources without express written approval from UC;
14. Prevent the storing, harvesting, or passing through of UC credentials (username, password, authentication secret, or other factor); and
15. Prevent the use or copying of Institutional Information for any purpose not authorized under the Agreement or any associated Statement of Work (SOW).

ARTICLE 5. REQUESTS FROM UC AND EVIDENCE OF COMPLIANCE

- A. Supplier must provide UC with evidence that demonstrates to UC's reasonable satisfaction Supplier's adherence to its information security plan (including but not limited to: third-party report, attestation signed by an authorized individual, attestation of compliance by a qualified assessor, or a mutually agreed upon equivalent) upon execution of the Agreement, upon reasonable request (including but not limited to: annually, after Major Changes, and/or as a result of a Security Incident), or as required by any applicable regulatory or governmental authority.
- B. Supplier must respond to UC's reasonable questions related to cybersecurity controls, Security Incidents, or Major Changes, newly published vulnerabilities, and/or risk assessments within ten (10) business days.
- C. UC may request and perform a security audit using a qualified third party or a mutually agreed upon alternative annually or as a result of a Breach.

ARTICLE 6. NOTIFICATION OF MAJOR CHANGES AND VULNERABILITY DISCLOSURES

- A. Within twenty (20) business days, Supplier must notify UC regarding changes in Supplier's security posture or IT infrastructure. Such notices must occur:
 1. When Major Changes happen.
 2. When Supplier becomes aware of a vulnerability that warrants a CVE² rating of "High" or "Critical," based on the latest CVE version, for which a patch is not yet available or for which Supplier will delay application of an available patch.
- B. Supplier must use commercially acceptable efforts to remediate, within twenty (20) business days, any vulnerability rated as CVE High or Critical.
- C. In response to Major Changes, Supplier must update its information security plan no later than fifteen (15) days into the next calendar quarter and must provide updated evidence of compliance with the information security plan.

² Common Vulnerabilities and Exposures (CVE) is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures maintained by The MITRE Corporation. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools. The CVE list can be found at: cve.mitre.org

ARTICLE 7. RETURN AND DISPOSAL OF INSTITUTIONAL INFORMATION

- A. Within thirty (30) calendar days of the termination, cancellation, expiration, or other conclusion of the Agreement, Supplier must return all Institutional Information to UC and then dispose of the Institutional Information in possession of Supplier as detailed herein. This provision also applies to all Institutional Information that is in the possession of sub-suppliers or agents of Supplier.
- B. Such disposal will be accomplished using the methods described in UC's Institutional Information Disposal Standard (<https://security.ucop.edu/policies/institutional-information-disposal.html>) or an alternative approved by UC.
- C. Supplier will certify in writing to UC that such return and/or disposal has been completed.
- D. If Supplier believes that return and/or disposal of Institutional Information is technically impossible or impractical, Supplier must provide UC with a written statement explaining the reason for this conclusion. If UC determines that return and/or disposal is technically impossible or impractical, Supplier will continue to protect the Institutional Information in accordance with the terms of this Appendix for as long as the Institutional Information is in Supplier's possession.

ARTICLE 8. NOTIFICATION OF CORRESPONDENCE CONCERNING INSTITUTIONAL INFORMATION

- A. Supplier agrees to notify UC promptly, both orally and in writing, but in no event more than seventy-two (72) calendar hours after Supplier receives correspondence or a complaint that relates to a regulation, contractual obligation, Breach, or material risk concerning Institutional Information. For purposes of this Article 8.A, a correspondence or complaint may include, but is not limited to, any communication that originates from law enforcement, regulatory or governmental agencies, government investigators, corporations, or an individual, but excludes normal customer service correspondence or inquiries.

ARTICLE 9. COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS

- A. **Reporting of Breach or Security Incident:** If Supplier reasonably suspects or confirms a Breach and/or a Security Incident impacting Institutional Information and/or IT Resources, Supplier must promptly notify UC both orally and in writing using the contacts in the Agreement. Supplier must provide such notifications no later than (1) seventy-two (72) calendar hours after the initial suspicion of a Security Incident and/or Breach and (2) seventy-two (72) calendar hours after the initial confirmation of a Security Incident and/or Breach, if Supplier is able to make such a confirmation. Supplier's notification must identify:
1. Contacts for both technical and management coordination;

2. Escalation and identifying information, such as ticket numbers, system identifiers, etc.;
 3. The nature of the Breach and/or Security Incident;
 4. The Institutional Information and/or IT Resources affected;
 5. What Supplier has done or will do to mitigate any deleterious effect; and
 6. What corrective action Supplier has taken or will take to prevent future Security Incidents.
- B. Supplier will provide other information as reasonably requested by UC.
- C. In the event of a suspected Breach and/or Security Incident, Supplier will keep UC informed regularly of the progress of its investigation until the incident is resolved.
- D. **Coordination of Breach Response or Security Incident Activities:** Supplier will fully cooperate with UC's investigation of any Breach and/or Security Incident involving Supplier and/or Goods and/or Services. Supplier's full cooperation will include, but not be limited to, Supplier:
1. Promptly preserving any potential forensic evidence relating to the Breach and/or Security Incident;
 2. Remediating the Breach and/or Security Incident as quickly as circumstances permit;
 3. Promptly, but no more than seventy two (72) calendar hours after the discovery of Breach and/or Security Incident, designating a contact person to whom UC will direct inquiries and who will communicate Supplier responses to UC inquiries;
 4. As rapidly as circumstances permit, assigning/using appropriate resources to remedy, investigate, and document the Breach and/or Security Incident, to restore UC service(s) as directed by UC, and undertake appropriate response activities;
 5. Providing status reports to UC regarding Breach and Security Incident response activities, either on a daily basis or a frequency approved by UC;
 6. Coordinating all media, law enforcement, or other Breach and/or Security Incident notifications with UC in advance of such notification(s), unless expressly prohibited by law;
 7. Ensuring that knowledgeable Supplier employees are available on short notice, if needed, to participate in UC and Supplier initiated meetings and/or conference calls regarding the Breach and/or Security Incident; and
 8. Ensuring that knowledgeable Supplier employees and agents participate in after-action analysis, including root cause analysis and preventive action planning.
- E. **Breaches and Security Incidents – Corrective And Preventive Action:** As a result of a Breach and/or Security Incident impacting Institutional Information and/or IT Resources, and upon UC's request, Supplier must prepare a report detailing corrective and preventive actions. The report must include:

1. A mutually agreed upon timeline for the corrective and preventive actions based on the nature of the Breach and/or Security Incident;
 2. Identification and description of the root causes; and
 3. Precise steps Supplier will take to address the failures in the underlying administrative, technical, and/or physical controls to mitigate damages and future cyber risk.
- F. **Costs:** Supplier must reimburse UC for reasonable costs related to responding to Breaches impacting Institutional Information and IT Resources caused by Supplier. This includes all costs associated with notice and/or remediation of the Breach.
- G. **Grounds for Termination:** Any Breach may be grounds for termination of the Agreement by UC. Agreement obligations to secure, dispose, and report continue through the resolution of the Breach and/or Security Incident.

ARTICLE 10. ILLICIT CODE WARRANTY

- A. Supplier represents and warrants that the Goods and/or Services do not contain Illicit Code.
- B. To the extent that any Goods and/or Services have Illicit Code written into them, Supplier will be in breach of this Agreement, and no cure period will apply.
- C. Supplier agrees, in order to protect UC from damages that may be intentionally or unintentionally caused by the introduction of Illicit Code, to promptly isolate or otherwise secure and then return Institutional Information and/or IT Resources.
- D. Supplier acknowledges that it does not have any right to electronically hold Institutional Information or assert any claim against UC by withholding the Goods and/or Services using Illicit Code.
- E. Should Supplier learn of the presence of Illicit Code, Supplier will promptly provide UC with written notice explaining the scope and associated risk.
- F. Supplier represents and warrants that it will take commercially reasonable steps to promptly remove Illicit Code.
- G. Supplier represents and warrants that even if Illicit Code is unintentionally installed via any method, Supplier will never utilize the Illicit Code.
- H. This provision does not relate to malware or viruses that attack the running IT Resource. These are covered under ARTICLE 9 - COORDINATING, REPORTING, AND RESPONDING TO BREACHES AND SECURITY INCIDENTS.

ARTICLE 11. BACKGROUND CHECKS

- A. Before Supplier's employee, sub-supplier, or agent may access Institutional Information and/or IT Resources classified at Protection Level 3 or Protection Level 4³, Supplier must conduct a thorough and pertinent background check. Supplier must evaluate the results prior to granting access in order to assure that there is no indication

³ See Exhibit 1.

that the employee, sub-supplier, or agent presents a risk to Institutional Information and IT Resources.

B. Supplier must retain each employee's, sub-supplier's, or agent's background check documentation for a period of three (3) years following the termination of the Agreement.

Exhibit 1 – Institutional Information

1. Protection Level Classification⁴:

- Protection Level 1
- Protection Level 2
- Protection Level 3
- Protection Level 4

Explanation:

The Protection Level determines the applicable cyber security insurance requirement in the Terms and Conditions.

2. Institutional Information data element descriptors:

Select all data types that apply:

- A. Animal Research Data.
- B. Controlled Technical Information (CTI).
- C. Controlled Unclassified Information (CUI) – 800-171/NARA.
- D. Defense Department: Covered Defense Information (CDI).
- E. Federal Acquisition Regulations (FARS/DFAR) other than CUI.
- F. GDPR personal data.
- G. GDPR special data.
- H. Health data – other identifiable medical data not covered by HIPAA. (Including but not limited to: occupational health, special accommodation, or services qualification, etc.)
- I. Health Records subject to HIPAA Privacy or Security Rule (PHI).
- J. Human Subject Research Data.
1. Identified.
2. Anonymized.
- K. Intellectual property (IP), such as patents, copyright, or trade secrets.
- L. ITAR/EAR-controlled data.
- M. Payment card data (PCI, PCI DSS).
- N. Personally identifiable information – PII.
- O. Student data, whether or not subject to FERPA.
- P. Other: _____
- Q. Other: _____

⁴ For reference see: <https://security.ucop.edu/policies/institutional-information-and-it-resource-classification.html>

- R. Other: _____
- S. Other: _____

3. Institutional Information Regulation or Contract Requirements:

Select all regulations or external obligations that apply to inform UC and the Supplier of obligations related to this Appendix:

Privacy (* indicates data security requirements are also present)

- A. California Confidentiality of Medical Information Act (CMIA) *.
- B. California Consumer Privacy Act (CCPA).
- C. California Information Practices Act (IPA).
- D. European Union General Data Protection Regulation (GDPR)*.
- E. Family Educational Rights and Privacy Act (FERPA) *.
- F. Federal Policy for the Protection of Human Subjects ("Common Rule").
- G. Genetic Information Nondiscrimination Act (GINA).
- H. Gramm-Leach-Bliley Act (GLBA) (Student Financial Aid) *.
- I. Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) *.
- J. Substance Abuse and Mental Health Services Administration SAMHSA (CFR 42 Part 2).
- K. The Fair and Accurate Credit Transaction Act (FACTA).
- L. The Fair Credit Reporting Act (FCRA).

Data Security

- M. Chemical Facility Anti-Terrorism Standards (CFATS).
- N. Defense Federal Acquisition Regulations (DFARS).
- O. Export Administration Regulations (EAR).
- P. Federal Acquisition Regulations (FARS).
- Q. Federal Information Security Modernization Act (FISMA).
- R. International Traffic in Arms Regulations (ITAR).
- S. Payment card data (PCI, PCI DSS).
- T. Toxic Substances Control Act (TSCA).
- U. Other: _____
- V. Other: _____
- W. Other: _____
- X. Other: _____

Exhibit 2

Spirion redacted Information Security Plan



Title: Corporate Information Security Policy	
Department: Corporate Information Security	Owner/Contact: Chief Information Security Officer
Approval Date: 10/29/2020	Last Review Date: 10/29/2020 Review Period: Annual
Applicability: All employees, contractors, and vendors of Spirion and its affiliated entities who access or use Spirion technology or who process or store Spirion data, irrespective of location.	
Authority: The Corporate Information Security Policy is enacted at Spirion under the direction of its Board of Directors.	

TABLE OF CONTENTS

1. INFORMATION SECURITY PROGRAM - PURPOSE	6
1.1 Introduction	6
1.2 Statement of Management Intent	6
1.3 Objectives.....	6
1.4 Information Security Policy Framework	7
1.5 Goals and Objectives.....	7
1.6 Focus Domains.....	8
1.7 Scope and Responsibility	9
2. INFORMATION SECURITY PROGRAM – POLICY & STANDARDS	ERROR!
BOOKMARK NOT DEFINED.	
2.1 Governance & Compliance	Error! Bookmark not defined.
2.1.1 Implementation	Error! Bookmark not defined.
2.1.2 Compliance Monitoring	Error! Bookmark not defined.
2.1.3 Exceptions	Error! Bookmark not defined.
2.1.4 Policy Modification.....	Error! Bookmark not defined.
2.1.5 Policy Review	Error! Bookmark not defined.
2.1.6 Governance Documentation Dissemination	Error! Bookmark not defined.
2.1.7 Payment Card Industry Data Security Standard (“PCI-DSS”)	Error! Bookmark not defined.
2.1.8 Gramm-Leach-Bliley Act.....	Error! Bookmark not defined.
2.1.9 Legal Compliance	Error! Bookmark not defined.
2.1.10 Open Issue Management	Error! Bookmark not defined.
2.1.11 Test, Monitor, Evaluate and Adjust the Corporate Information Security Policy.....	Error!
Bookmark not defined.	
2.1.12 Questions, Feedback and Reporting Violations	Error! Bookmark not defined.
2.1.14 Governance Structure & Responsibilities	Error! Bookmark not defined.
2.1.15 Copyright and Intellectual Property Compliance	Error! Bookmark not defined.
2.2 System Development & Maintenance	Error! Bookmark not defined.

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.

2.2.1	Production Data and Test/Development Environments	Error! Bookmark not defined.
2.2.2	System Design.....	Error! Bookmark not defined.
2.2.3	System Testing & Acceptance	Error! Bookmark not defined.
2.2.4	System Implementation.....	Error! Bookmark not defined.
2.2.5	System Decommissioning	Error! Bookmark not defined.
2.2.6	Internet Accessible System Deployment.....	Error! Bookmark not defined.
2.2.7	Capacity Planning	Error! Bookmark not defined.
2.2.8	Processing Validation.....	Error! Bookmark not defined.
2.2.9	Control of Application Software	Error! Bookmark not defined.
2.2.10	Access Control to Application Source Library.....	Error! Bookmark not defined.
2.3	Access Control	Error! Bookmark not defined.
2.3.1	Separation of Duties	Error! Bookmark not defined.
2.3.2	Access Control and Authorization	Error! Bookmark not defined.
2.3.3	Passwords.....	Error! Bookmark not defined.
2.3.4	Access Control Strategies.....	Error! Bookmark not defined.
2.3.5	Validating User Access to Business Applications.....	Error! Bookmark not defined.
2.3.6	Validating User Access to Non-Application Platforms.....	Error! Bookmark not defined.
2.3.7	Administrative Privileges	Error! Bookmark not defined.
2.3.8	Authentication	Error! Bookmark not defined.
2.3.9	Delegation of Information Security Administration.....	Error! Bookmark not defined.
2.3.10	Documentation of Access Changes	Error! Bookmark not defined.
2.3.11	System Access Approvals	Error! Bookmark not defined.
2.3.12	Personnel Termination and Transfers Access Changes.....	Error! Bookmark not defined.
2.3.13	Remote Access	Error! Bookmark not defined.
2.3.14	End User and Privileged Remote Access	Error! Bookmark not defined.
2.3.15	File Transfer Process Authentication	Error! Bookmark not defined.
2.3.16	Access to Voice Messages	Error! Bookmark not defined.
2.3.17	Logon Account Issuance	Error! Bookmark not defined.
2.3.18	Default Accounts.....	Error! Bookmark not defined.
2.3.19	Account Provisioning.....	Error! Bookmark not defined.
2.3.20	Third-Party Access Limitation	Error! Bookmark not defined.
2.4	Business Continuity & Operational Resilience	Error! Bookmark not defined.
2.4.1	Environmental Hazards and Technological Failures.....	Error! Bookmark not defined.
2.4.2	Business Continuity Planning	Error! Bookmark not defined.
2.4.3	Backup and Retention	Error! Bookmark not defined.
2.4.4	Pandemic Response.....	Error! Bookmark not defined.
2.4.5	Order of Succession and Delegation of Authority.....	Error! Bookmark not defined.
2.5	Change Control & Configuration Management.....	Error! Bookmark not defined.
2.5.1	Change Management.....	Error! Bookmark not defined.

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



2.5.2	Change Impact Analysis.....	Error! Bookmark not defined.
2.5.3	Change Approval and Implementation.....	Error! Bookmark not defined.
2.5.4	Emergency Changes.....	Error! Bookmark not defined.
2.5.5	End-of-life Products.....	Error! Bookmark not defined.
2.5.6	Modifications to Customer Information Systems.....	Error! Bookmark not defined.
2.5.7	Communication of Changes to Procedures.....	Error! Bookmark not defined.
2.5.8	Baseline Configuration Management.....	Error! Bookmark not defined.
2.5.9	Host Security.....	Error! Bookmark not defined.
2.5.10	Unattended Workstations.....	Error! Bookmark not defined.
2.5.11	Session Time-out.....	Error! Bookmark not defined.
2.5.12	Remote Control Software.....	Error! Bookmark not defined.
2.6	Data Security & Information Lifecycle Management.....	Error! Bookmark not defined.
2.6.1	Document Disposal Services.....	Error! Bookmark not defined.
2.6.2	Data Masking.....	Error! Bookmark not defined.
2.6.3	Information Data Classification.....	Error! Bookmark not defined.
2.6.4	Protection of PII.....	Error! Bookmark not defined.
2.6.5	Protection of Off-System Financial Statement Files.....	Error! Bookmark not defined.
2.6.6	Transmission of Sensitive Information.....	Error! Bookmark not defined.
2.6.8	Transmitting Sensitive or Private Data.....	Error! Bookmark not defined.
2.6.9	Destruction of Printed Information, Electronic Data and Other Storage Media.....	Error! Bookmark not defined.
2.6.10	Destruction Requirements for Computer Storage Media.....	Error! Bookmark not defined.
2.6.11	Datacenter Authorization.....	Error! Bookmark not defined.
2.6.12	Data Retention.....	Error! Bookmark not defined.
2.7	Asset Management.....	Error! Bookmark not defined.
2.7.1	Information Stewardship.....	Error! Bookmark not defined.
2.7.2	Use of 3 rd Party Software and Equipment.....	Error! Bookmark not defined.
2.7.3	Asset Inventory.....	Error! Bookmark not defined.
2.7.4	Use of Off-Site Equipment.....	Error! Bookmark not defined.
2.7.5	Equipment Disposal.....	Error! Bookmark not defined.
2.8	Encryption & Key Management.....	Error! Bookmark not defined.
2.8.1	Encryption Requirements.....	Error! Bookmark not defined.
2.8.2	Password Hashing.....	Error! Bookmark not defined.
2.8.3	Digital Signatures.....	Error! Bookmark not defined.
2.8.4	Selecting and Using Passwords for Use with Encryption Tools ...	Error! Bookmark not defined.
2.8.5	Protection of Cryptographic Keys.....	Error! Bookmark not defined.
2.8.6	Key Escrow.....	Error! Bookmark not defined.
2.8.7	Use of Cryptographic Keys.....	Error! Bookmark not defined.
2.8.2	Symmetric Key Management.....	Error! Bookmark not defined.

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



2.8.3 Asymmetric Key Management.....	Error! Bookmark not defined.
2.8.4 Approved Algorithms.....	Error! Bookmark not defined.
2.9 Risk Management.....	Error! Bookmark not defined.
2.9.1 Effort-Level Risk Assessments	Error! Bookmark not defined.
2.9.2 Enterprise Risk Assessment	Error! Bookmark not defined.
2.9.3 Cyber Insurance	Error! Bookmark not defined.
2.10 Organizational Security Responsibilities	Error! Bookmark not defined.
2.10.1 Use of Technology and Information Assets	Error! Bookmark not defined.
2.10.2 Acceptable Use of Information Technology	Error! Bookmark not defined.
2.10.3 Bring Your Own Device (BYOD).....	Error! Bookmark not defined.
2.10.4 Electronic Mail Usage.....	Error! Bookmark not defined.
2.10.5 Monitoring of Email Communications.....	Error! Bookmark not defined.
2.10.6 Retention and Archiving of Electronic Mail	Error! Bookmark not defined.
2.10.7 Internet Usage	Error! Bookmark not defined.
2.10.8 Internet Access	Error! Bookmark not defined.
2.10.9 Internet Usage Individual Responsibility	Error! Bookmark not defined.
2.10.10 Security Awareness Training	Error! Bookmark not defined.
2.10.11 Employee Onboarding.....	Error! Bookmark not defined.
2.10.12 No Expectation of Privacy	Error! Bookmark not defined.
2.10.13 Termination of Employment	Error! Bookmark not defined.
2.10.14 Use of Cloud Services	Error! Bookmark not defined.
2.11 Logging & Monitoring	Error! Bookmark not defined.
2.11.1 Security Auditing Logging and Review	Error! Bookmark not defined.
2.11.2 Security Details	Error! Bookmark not defined.
2.11.3 External Disclosure of Security Audit Logs.....	Error! Bookmark not defined.
2.11.4 Security Audit Log Retention.....	Error! Bookmark not defined.
2.11.5 Security Monitoring	Error! Bookmark not defined.
2.11.6 Data Loss Prevention	Error! Bookmark not defined.
2.12 Incident Management	Error! Bookmark not defined.
2.12.1 Investigations and Incident Response	Error! Bookmark not defined.
2.12.2 Incident Response Process	Error! Bookmark not defined.
2.12.3 Collection of Evidence	Error! Bookmark not defined.
2.12.4 Post-Incident Analysis.....	Error! Bookmark not defined.
2.12.5 Periodic Testing	Error! Bookmark not defined.
2.13 Third Party Management	Error! Bookmark not defined.
2.13.1 Vendor Assurance Monitoring	Error! Bookmark not defined.
2.13.2 Confidentiality and Non-Disclosure Agreements.....	Error! Bookmark not defined.
2.13.3 Exchange Agreements.....	Error! Bookmark not defined.
2.13.4 Subsidiary and Affiliate Access and Network Connectivity	Error! Bookmark not defined.

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



2.13.5	Oversee Service Providers That Access Customer Information..	Error! Bookmark not defined.
2.13.6	Third Party Data & Information Exchange	Error! Bookmark not defined.
2.13.7	Divestiture Protection.....	Error! Bookmark not defined.
2.13.8	Joint Ventures, Mergers and Acquisitions.....	Error! Bookmark not defined.
2.13.9	Outsourced Application Development	Error! Bookmark not defined.
2.14	Physical & Environmental Security	Error! Bookmark not defined.
2.14.1	General Responsibilities.....	Error! Bookmark not defined.
2.14.2	Facility Security	Error! Bookmark not defined.
2.14.3	Clean Desk	Error! Bookmark not defined.
2.14.4	International Travel.....	Error! Bookmark not defined.
2.14.5	Computer Room and Data Security.....	Error! Bookmark not defined.
2.14.6	Recording of Audio/Video	Error! Bookmark not defined.
2.14.7	Wireless Technology.....	Error! Bookmark not defined.
2.14.8	Home Office Security.....	Error! Bookmark not defined.
2.14.9	Security Perimeters	Error! Bookmark not defined.
2.14.10	Parking Area Security	Error! Bookmark not defined.
2.14.11	Environmental Protection.....	Error! Bookmark not defined.
2.14.12	Server Room Security	Error! Bookmark not defined.
2.14.13	Emergency Response	Error! Bookmark not defined.
2.14.14	Site Closures.....	Error! Bookmark not defined.
2.14.15	Physical Access Control.....	Error! Bookmark not defined.
2.15	Network Security.....	Error! Bookmark not defined.
2.15.1	Environment Isolation.....	Error! Bookmark not defined.
2.15.2	Firewall Technology	Error! Bookmark not defined.
2.16	Threat & Vulnerability Management.....	Error! Bookmark not defined.
2.16.1	Virus Detection and Prevention	Error! Bookmark not defined.
2.16.2	Intrusion Detection & Prevention.....	Error! Bookmark not defined.
2.16.3	Patch and Vulnerability Management	Error! Bookmark not defined.
2.16.4	Security Testing	Error! Bookmark not defined.
2.16.5	Penetration Testing.....	Error! Bookmark not defined.
2.16.6	Threat Information Sharing.....	Error! Bookmark not defined.
	DEFINITIONS	ERROR! BOOKMARK NOT DEFINED.
	KEY ROLES & RESPONSIBILITIES	ERROR! BOOKMARK NOT DEFINED.
	REFERENCE MATERIAL.....	ERROR! BOOKMARK NOT DEFINED.
	RELATED POLICIES AND PROCEDURES.....	ERROR! BOOKMARK NOT DEFINED.
	RELATED REGULATIONS.....	ERROR! BOOKMARK NOT DEFINED.

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



1. Information Security Program - Purpose

1.1 Introduction

Spirion's Information Security Program is the trust foundation upon which customer relationships are built. It is designed to support and augment Spirion's focus on agility and cost-management while balancing strong risk management practices to deliver a level of assurance that meets or exceeds the standards of its customers. The hallmarks of Spirion are its people, processes, innovation, and technology. Accordingly, the Information Security Program is the culmination of the organizational governance that defines the on-going assurance requirements and obligations pertaining to each of these aspects of Spirion. This governance prescribes the manner in which the Company conducts its operations in order to preserve the confidential information in which Spirion has been entrusted to protect and the intellectual property that delivers Spirion's competitive advantages.

1.2 Statement of Management Intent

Spirion is committed to ensuring the availability, integrity, and confidentiality of the information entrusted to it by its stakeholders including management, staff, investors, clients, and other business partners.

Spirion management is accountable for setting, enforcing, and supporting the Policies and Standards surrounding security of information and information-related assets. The responsibility for maintaining and supporting security, however, is implicit in the roles and daily duties of all Spirion employees, temporary workers, consultants, and contractors, hereafter referred collectively as "Spirion staff."

Spirion's philosophy on security is further defined and embodied in the Corporate Information Security Program. This document includes principles governing the following Key Control areas:

- Governance and Compliance
- System Development and Maintenance
- Access Control
- Business Continuity and Operational Resilience
- Change Control and Configuration Management
- Data Security and Information Lifecycle Management
- Asset Management
- Encryption and Key Management
- Risk Management
- Organizational Security Responsibilities
- Logging and Monitoring
- Incident Management
- Third-Party Management
- Physical and Environmental Security
- Network Security
- Threat and Vulnerability Management

Spirion's Security Policies are consistent with the Spirion culture and organizational risk tolerances, and address other applicable internal and external requirements.

1.3 Objectives

Spirion, its subsidiaries and affiliates (collectively, including subsidiaries and affiliates, sometimes referred to herein as the "Company"), recognizes the critical importance of maintaining a comprehensive, industry standard Corporate Information Security Policy ("CISP") to safeguard information, whether it be non-public personal information ("NPI"), Payment Card Industry ("PCI") cardholder information ("CHI"), Protected Health Information ("PHI"), personally identifiable information of its clients and workforce (collectively, including all individually identifiable information, sometimes referred to herein as "PII"), or other information that is proprietary to the

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



Company.

This document describes the Spirion Information Security Program and contains approved Corporate Information Security policy statements governing people, practices, technology, supplemental policies, subordinate programs, standards, procedures, training, and other related programs.

This CISP includes administrative, technical, and physical safeguards designed to achieve the following objectives, taking into consideration the sensitivity of the information intended to be safeguarded as well as the complexity and scope of Spirion's activities:

- 1) Ensure the security, confidentiality, integrity and availability of information – includes NPI, PII, and other forms of confidential Company information;
- 2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- 3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or individual, or to the Company;
- 4) Ensure the proper disposal of PII, customer information and consumer information;
- 5) Provide reasonable assurance that business objectives will be achieved and security breaches will be prevented or detected, contained and corrected; and
- 6) Comply with legal, statutory, contractual, and internally developed requirements (including, without limitation, the Gramm-Leach-Bliley Act).

Whether the obligations described herein are performed internally or by a trusted partner, the same risk management rigors and oversight shall be employed. The outsourcing of any service does not relieve Company management of responsibility to ensure the design, management, implementation and execution of appropriate security practices nor does it alleviate any risk management obligations expected of Spirion by its customers.

1.4 Information Security Policy Framework

Spirion's Information Security Policy Framework consists of policies, programs, standards and procedures. This document establishes the conceptual and sometimes specific qualities that establish the assurance auspices within which the operations of the company occur. This framework ensures that risks are well-understood by the appropriate audiences and that controls to prevent or limit harm to the company or its information assets are established and functioning as intended. In order to establish applicability across all germane aspects of the company, subordinating policies, standards, guidelines, and procedures may be developed to further refine the aspirations contained herein.

The Director of Operational and Information Security Risks (DOISR) is responsible for administering the CISP. In addition, the DOISR is responsible for managing the program and developing, implementing and enforcing the program's policy statements. The DOISR shall provide periodic reports regarding the status of the program and the overall state of Company security to Senior Management, the Corporate Compliance Committee, and the Spirion Board of Directors and the Finance and Operations Committee thereof as may be necessary or appropriate.

1.5 Goals and Objectives

The objective of the CISP is to define the guiding principles, requirements and framework used to maintain the confidentiality, integrity and availability of Spirion information resources. The goal of the program is to properly secure all Company information assets while still facilitating the access needed for the business to run smoothly and efficiently. This goal is accomplished by implementing mechanisms and controls to ensure Spirion data is protected in accordance with all applicable laws and regulations.

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



Availability refers to the assurance that reliable and timely access to data and resources is granted to authorized individuals. Controls must be in place to ensure that Spirion information systems:

- Provide adequate capacity in order to perform in a predictable manner with an acceptable level of performance;
- Are able to recover from disruptions in a secure and timely manner so that client productivity is not negatively affected;
- Avoid single points of failure by implementing redundancy mechanisms when necessary; and
- Implement necessary mechanisms to protect against inside and outside threats that could affect the availability and productivity of the system.

Confidentiality refers to the assurance that access to information is restricted to only authorized users. Confidentiality applies to data in both electronic and physical forms and must be maintained while data is at rest and in transmission. Spirion has policies and procedures in place to protect the confidentiality of data utilizing methods that include strong authentication mechanisms, strict access control, air-gapped network boundaries, proper use of encryption, and employee education.

Integrity refers to the assurance that information is accurate and reliable and that controls are in place to prevent the unauthorized modification of information or data. Hardware, software and communications mechanisms must work in a concerted manner to maintain and process data correctly and move data to intended destinations without unexpected alteration. Controls are implemented to ensure that information systems are protected from integrity-related threats that originate from external sources.

To help ensure the integrity of Spirion systems and data, policies and procedures are in place to restrict access to systems to authorized users, prevent unauthorized activity by authorized users and maintain separation of duties. Policies and procedures are in place to govern the implementation of new systems and changes made to existing systems. Emplaced technical controls monitor critical assets to detect various attacks on integrity within technology resources.

1.6 Focus Domains

Appropriate security controls focus on the following domains or areas of protection:

- Management and administration processes that address security-related programs, policies, standards, procedures, staffing, monitoring, training and end user education in order to ensure effective controls are in place and that continual maintenance and administration of these controls exists at an appropriate level;
- Communication Processes that address the internal and external transmission of information in order to ensure that appropriate levels of protection exist to safeguard the transmission of information, the integrity of data and to prevent the disclosure of sensitive information;
- Hardware Resources and Devices (virtual or physical) that ensure appropriate levels of protection exist to prevent unauthorized access, modification or compromise to these components. Hardware resources may include:
 - Network and telecommunication devices including, but not limited to, routers, firewalls, gateways, network switches, modems, private branch exchange (“PBX”) systems, telecom switches, voice mail systems and access servers;

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



- Processing systems including, but not limited to, network and database servers, file and print servers, mail servers, Internet servers, backup systems;
 - Individually assigned systems including, but not limited to, stand-alone computers and peripherals such as workstations, laptops, handheld devices, tablets, modems, hard drives, removable drives, disks and tapes;
 - Development servers and workstations, stand-alone networks used for research and development (R&D), and isolated labs or testing areas, system development and analysis; and
 - Printers and fax machines.
-
- Operating System, Database, Software and Application Resources in order to protect the security, functionality, confidentiality, integrity and availability of these items to ensure reliability, uninterrupted processing and appropriate access;
 - Operational Processes that address the protection of manual or non-automated functions that support the data processing environment or support end user computing, including troubleshooting, software distribution, computer resource inventories, print output, paper copy information and the routing, storage and destruction of this information;
 - Physical Security to ensure adequate protection measures have been implemented to safeguard servers, convergence devices, workstations, paper records and files, other print media, the data processing center, telecommunications and network rooms, off-site storage locations, workspaces and all areas where workstations and servers connected to the network are located; irrespective of whether Spirion is the physical custodian of devices or a trusted third-party is engaged in this capacity
 - Business Continuity, Disaster Recovery and Contingency Planning to ensure adequate plans exist that provide for the resumption and continued functioning of vital and critical services and processes of the organization during emergencies or disaster situations; and
 - Legal and Compliance to ensure controls, review processes and protection strategies are in place to safeguard PII, whether in paper, electronic or other form; including but not limited to individual consumer and customer NPI.

1.7 Scope and Responsibility

The CISP and related governing requirements are further realized through the Company's leadership, Information Security Risk Management distributed responsibility, and shared-risk model.

Business unit and staff department heads are responsible for:

- All information assets acquired or created by personnel within their respective organizations;
- The computer resources, application systems and information outputs from those systems that are located within their respective organizations; and
- Ensuring that the relevant laws, regulations and information security governing requirements are implemented to protect these assets, and that all personnel within their respective organizations adhere to them.

FOR INTERNAL USE ONLY

Note: Printed copies of this document are for reference only. The official version of this document is available on the corporate intranet site. It is not to be delivered to third parties for off-site review.



UNIVERSITY OF CALIFORNIA

Appendix – Business Associate Agreement

This Appendix - Business Associate Agreement ("Appendix BAA") supplements and is made a part of any and all agreements entered into by and between The Regents of the University of California, a California corporation ("UC"), on behalf of its University of California Health System and _____, Business Associate ("BA").

RECITALS

- A. UC is a "Covered Entity" as defined under 45 C.F.R. § 160.103
- B. UC and BA are entering into or have entered into, and may in the future enter into, one or more agreements (each an "Underlying Agreement") under which BA performs functions or activities for or on behalf of, or provides services to UC ("Services") that involve receiving, creating, maintaining and/or transmitting Protected Health Information ("PHI") of UC as a "Business Associate" of UC as defined under 45 C.F.R. § 160.103. This Appendix BAA shall only be operative in the event and to the extent this Appendix BAA is incorporated into an Underlying Agreement between UC and BA.
- C. UC and BA desire to protect the privacy and provide for the security of PHI used by or disclosed to BA in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the regulations promulgated thereunder by the U.S. Department of Health and Human Services (45 C.F.R. Parts 160, 162 and 164) (the "HIPAA Regulations"), the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"), California Civil Code § 56 et seq., §§1798.82 and 1798.29, and other applicable laws and regulations. The purpose of this BA Agreement is to satisfy certain standards and requirements of HIPAA, the HIPAA Regulations, including 45 CFR § 164.504(e), the HITECH Act, including Subtitle D, part 1, as they may be amended from time to time, and similar requirements under California law.
- D. UC has designated all of its HIPAA health care components as a single component of its hybrid entity and therefore this BA Agreement is binding on all other UC health care components (collectively, the Single Health Care Component or the SHCC). This BA Agreement is effective on the date of the Underlying Agreement under which BA provides Services to UC ("Effective Date").

1. DEFINITIONS

Except for PHI, all capitalized terms in this Appendix BAA shall have the same meaning as those terms in the HIPAA Regulations.

PHI shall have the same meaning as "protected health information" in the HIPAA Regulations that is created, received, maintained, or transmitted by Business Associate or any Subcontractor on behalf of UC and shall also include "medical information" as defined at Cal. Civ. Code § 56.05.

2. OBLIGATIONS OF BA

BA agrees to:

- A. Comply with the requirements of the Privacy Rule that apply to UC in carrying out such obligations, to the extent BA carries out any obligations of UC under the Privacy Rule. BA also agrees to comply with the requirements of California state privacy laws and regulations that apply to UC in carrying out such obligations, to the extent BA carries out any obligations of UC under California Civil Code § 1798 et seq., California Civil Code § 56 et seq., and California Health & Safety Code §§ 1280.15 and 1280.18, as applicable, unless otherwise mutually agreed to by BA and UC.
- B. Not Use or Disclose PHI other than as permitted or required by the Underlying Agreement or as required by law.
- C. Use appropriate safeguards, and comply, where applicable, with 45 C.F.R. § 164 Subpart C with respect to ePHI, to prevent the Use or Disclosure of PHI other than as provided for by the Underlying Agreement(s) and the Appendix BAA.
- D. Notify UC, orally and in writing, as soon as possible, but in no event more than five (5) calendar days, after BA becomes aware of any Use or Disclosure of the PHI not permitted or required by the Appendix BAA or Underlying Agreement(s), including Breaches of unsecured PHI as required by 45 C.F.R. § 164.410 and potential compromises of UC PHI, including potential inappropriate access, acquisition, use or disclosure of UC PHI (each, collectively an “Incident”). BA shall be deemed to be aware of any such Incident, as of the first day on which it becomes aware of it, or by exercising reasonable diligence, should have been known to its officers, employees, agents or sub-suppliers. The notification to UC shall include, to the extent possible, each individual whose unsecured PHI has been, or is reasonably believed by BA to have been, accessed, acquired, used or disclosed during such Incident. BA shall further provide UC with any other available information that UC is required to include in a notification to affected individuals at the time of the notification to UC, or promptly thereafter as information becomes available. BA shall take prompt corrective action to remedy any such Incident, and, as soon as possible, shall provide to UC in writing: (i) the actions initiated by the BA to mitigate, to the extent practicable, any harmful effect of such Incident; and (ii) the corrective action BA has initiated or plans to initiate to prevent future similar Incidents.
- E. Ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same restrictions, conditions, and requirements that apply to the BA with respect to such PHI.
- F. If BA maintains PHI in a Designated Record Set, BA shall make the PHI in the Designated Record Set available to UC, or if directed by UC to the Individual or the Individual’s designee, as necessary to satisfy UC’s obligations under 45 C.F.R. § 164.524.
- G. If BA maintains PHI in a Designated Record Set, BA shall make any amendments directed or agreed to by UC pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy UC’s obligations under 45 C.F.R. § 164.526.

- H. Maintain and make available the information required to provide an accounting of disclosures to UC, or if directed by UC to the Individual, as necessary to satisfy UC’s obligations under 45 C.F.R. § 164.528.
- I. 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 UC’s compliance with HIPAA, HITECH and their implementing regulations.

3. PERMITTED USES AND DISCLOSURES BY BA

BA may only Use or Disclose the Minimum Necessary PHI to perform the services set forth in the Underlying Agreement.

4. TERM AND TERMINATION

- A. Termination for Cause. UC may terminate this Appendix BAA and any Underlying Agreement(s), if UC determines BA has violated a material term of the Appendix BAA.
- B. Upon termination of this Appendix BAA for any reason, with respect to PHI received from UC, or created, maintained, or received by BA on behalf of UC, BA shall return to UC, or if agreed to by UC, destroy, all such PHI that BA still maintains in any form, and retain no copies of such PHI.


To the extent return or destruction of UC PHI is not feasible, BA shall (1) retain only that PHI which is necessary for BA to continue its proper management and administration or to carry out its legal responsibilities; and (2) continue to use appropriate safeguards for such UC PHI and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI to prevent Use or Disclosure of the PHI, other than as provided for in this Section, for as long as BA retains the PHI.

- C. Survival. The obligations of BA under this Section 4.B shall survive the termination of this Appendix BAA and any Underlying Agreement(s).

The Appendix BAA is signed below by the parties’ duly authorized representatives.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

SPIRION LLC



 (Signature)

Paul Williams, Chief Procurement Officer
 (Printed Name, Title)

August 10, 2021

 (Date)

(Supplier Name)


 (Signature)

Tom Palomaki

 (Printed Name, Title)

11/4/2021

 (Date)

Attachment B to Purchase Agreement #
Customer Support Services and Service Level Agreement

A. Support and Maintenance

1. As long as Customer continues to pay its Annual Subscription Fee, Spirion will provide maintenance, support, new releases and product upgrades to the products set forth in the applicable Quote.
2. Spirion will conduct regular maintenance. Spirion's standard maintenance window will be 9 AM to 6 PM ET Monday to Saturday. In the event maintenance is required outside the normal maintenance hours, Spirion will provide Customer with 24 hours' notice of the maintenance window.
3. All new releases and product updates made generally available to other Spirion customers using the System will be installed and configured as necessary during the term of this Agreement by Spirion. Customizations, product upgrades, or enhancements specifically tailored to Customer may be provided for an additional fee as set forth in an Order Form. Determination of whether specific modifications are customizations, upgrades, or enhancements will be made solely and exclusively by Spirion.
4. There will be no reductions in the functionality set forth in any Documentation unless the parties mutually agree otherwise.
5. Customer support is provided Monday through Friday from 9AM to 6PM ET, except during U.S. national holidays. Customer may request support by entering a support ticket with all technical user queries or issues on the Spirion Customer Success Center portal at <https://myguide.spirion.com/>. Customer should include contact information and a detailed description of the issue in the ticket. A support representative will respond with either a resolution or workaround, either by email or phone, as warranted by the ticket, within a 24-hour period. In the event that an issue is not resolved within the 24-hour period, Customer should promptly contact Spirion.

B. Service Levels

1. *Definitions.*
 - a. **"Availability"** means (total uptime minutes of the System in the month / (total minutes in month – total Maintenance minutes - any Excused Downtime minutes)) x 100, where Maintenance minutes equals the time taken for regular maintenance as defined in A.2.
 - b. **"Defect"** means any failure of the System to conform to the Documentation;

- c. **“Excused Downtime”** means the total minutes in the month during which the System was not available due to (a) any negligent or wrongful act or omission by Customer or its users; (b) any negligent or wrongful act or omission by Third-Party Vendors; or (c) any force majeure events or disruption in public internet access.
 - d. **“Severity Level 1 (Critical Impact)”** means a Defect resulting in the loss of service, or critical business functions with no possible bypass, recovery, or other Workaround. All Severity Level definitions and assignments are determined solely by Spirion. For a Severity Level 1 problem, a Defect must severely impact production to a point where work cannot continue until the problem is resolved. If resolution requires a software fix, it may be delivered outside of the normal release cycle for issues that cannot be resolved or worked around until the next release is deployed;
 - e. **“Severity Level 2 (Major Impact)”** means a Defect where production is significantly impacted or degraded. For a Severity Level 2 problem, the Software is impaired, but Customer can perform critical business functions and no data is being corrupted. If resolution requires a software fix, it may be delivered outside of the normal release cycle for issues that cannot be resolved or worked around until the next release is deployed;
 - f. **“Severity Level 3 (Minor Impact)”** means any Defect (i) that does not fall into the categories of Severity Level 1 or Severity Level 2 problems, or (ii) that was previously categorized as a Severity Level 1 or Severity Level 2 problem, or still exists as a result of such problems, but for which Spirion provided an acceptable Workaround. If resolution requires a software fix, such resolutions will be addressed in a generally-available release. The scheduling of software fixes and releases will be determined by Spirion; and
 - g. **“Workaround”** means a temporary or permanent solution to a Defect that allows the Software to regain functionality in accordance with the Documentation, or reduces the severity of the Defect.
2. Spirion, with Customer's reasonable assistance, will work diligently to resolve each Severity Level 1 problem or implement an acceptable Workaround within twenty-four (24) clock hours after Spirion receives notice of such problem.
 3. Spirion, with Customer's reasonable assistance, will work diligently to resolve each Severity Level 2 problem or implement an acceptable Workaround within forty-eight (48) clock hours after Spirion receives notice of such problem.
 4. Spirion will resolve Severity Level 3 problems or implement an acceptable Workaround in a future generally available release or otherwise upon a schedule determined by Spirion.

5. Spirion will ensure an Availability of the Software of 99%, twenty-four (24) hours per day, seven (7) days per week, including all legal holidays during the Term of the Agreement.
6. If Spirion fails to comply with the provisions of Sections B.2, B.3 or B.5 above (relating to Severity Level 1 and Severity Level 2 problems and Availability failures) more than three (3) times in a single calendar month, Spirion will refund to Customer an amount equal to one-twelfth (1/12) of the annual License Fee, but only to the extent Customer paid Spirion such License Fees pursuant to the most recent quarterly invoice which was due and payable. The remedies set forth in this Section B.6 constitute Customer's sole and exclusive remedies for any breach of or noncompliance with the service level agreements set forth in this Section B.

C. Service Level Exceptions

7. Spirion will not be responsible for failure to meet any SLA metric to the extent that the failure is affected or caused in whole or in part by (a) Customer's failure to perform its material obligations, as set forth in a binding agreement in place, or (b) any other cause beyond Spirion Control. The period of time that services are interrupted due to the conditions listed below will be excluded from SLA performance calculations for relevant cases:
 - a. Customer's failure to meet its obligations set forth in this SOW or the Agreement for the applicable Service;
 - b. Problems resulting from components (eg: hardware, software, network, maintenance) for which Customer or any other party is responsible.
 - c. Problems caused by the actions or inactions of Customer's personnel, other third party providers to Customer, or Customer's infrastructure, including, but not limited to, misconduct, negligent acts or omissions, inaccurate or incomplete information, or any unauthorized modifications made to any managed hardware or software devices by Customer or any of its agents, employees, contractors, consultants, end users, or any other third parties acting on behalf of Customer.
 - d. Customer's material impediment of Spirion's efforts to meet the SLAs.
 - e. Scheduled maintenance, alteration, or implementation.
 - f. Customer tool latency issues or planned or unplanned outages.
 - g. Software manufacturer "bug" related problems requiring third-party involvement.
 - h. Data restoration.
 - i. Virus attacks to the extent unrelated to the fault or negligence of Spirion.
 - j. Customer provision of inaccurate or incomplete information or failure to provide previously agreed upon required information.
 - k. Customer's prioritization of available Spirion resources.
 - l. All Hands on Deck type of incidents, defined as events where all or a substantial portion of Spirion staff is required to handle a Customer emergency issue.
 - m. Any transport or appliance faults.



News and Announcements
Here you will find Spirion Support News, Product Announcements, Release Notes, and FAQs.

Knowledge Base
Learn a skill, How To Guides for Search Locations, Troubleshooting, and More...

Implementing Spirion
This section will help new customers, customers in implementation or, wishing to refresh Spirion.

Promoted articles

- FAQ: Searching MYSQL Connector That Requires TLS 1.2
- FAQ: Big Sur showing an Error that the Endpoint Service is Damaged
- Notice: Deprecation of TLS 1.0 and 1.1 for SMTPS
- FAQ: JAMF Deployments Causing an Error
- FAQ: Big Sur Support
- How Do I Send a Feature Request to Spirion?
- How To View/Update Existing Spirion Tickets
- Links to User Guides, Documentation, and Feedback
- Test/Sample Data

Release Notes

- Console Release Notes
- Windows Client - Endpoint Release Notes
- Mac Client - Endpoint Release Notes
- Linux Client - Endpoint Release Notes

News and Announcements

Here you will find Spirion Support News, Product Announcements, Release Notes, and FAQs.

Hot Topics

- FAQ: Big Sur Support
- How Do I Send a Feature Request to Spirion?
- Working From Home Frequently Asked Questions

Support News and Announcements

- Notice: Deprecation of TLS 1.0 and 1.1 for SMTPS
- How To View/Update Existing Spirion Tickets
- 11.8 Releases
- 11.7.1 Release Announcement
- 11.5 Releases
- 11.4 Releases
- See all 9 articles

Using Support

What Issues are Covered by Support?

Spirion's support department generally handles three types of issues :

- **Break/Fix - Contact Support** when your console and or endpoint are not behaving in ways that are expected. I.E. cannot log in to the console, searches are not being distributed, endpoints are not communicating ect. When a ticket is opened with support please provide a **gathered data** so that support may assist you in a timely fashion.
- **Defects - Contact Support** after it has been confirmed that a setting is configured as per the documentation but the application is not performing as described. Also, if a replicable bug is identified, Spirion generates an error report, or the operating system reports a crash. And also, when using Spirion for its intended purpose and it stops responding for a long period of time or unexpectedly closes without generating errors.
- **Incorrect/Missing Documentation - Contact Support** when the specific steps as detailed in existing documentation have been followed exactly, but the application is not performing as described. Additionally, if documentation for a feature or function does not exist, please let us know where the information was expected so that our documentation team may create the necessary content in a location intuitive for our customers.

In the cases above, please open a support ticket and provide as much relevant information as possible such as the exact configuration and steps performed including any application log files. If there is a relevant KB article, please detail what occurred after the documented resolution was attempted so that our support team can provide timely and effective responses.

Support Hours

Support Analysts are available from 8 am to 6 pm (EST/EDT) M - F excluding holidays.

Support Response Times

Our support engineers are among the fastest in the industry with approximately 60 percent of tickets responded to within an hour. Generally, you can expect a response from the support engineers within four hours during the support hours posted above. On very rare occasions it may take longer to respond to your ticket. Please wait up to 24 hours (1 business day) before contacting Support about the same issue.

Premium Support Offerings

Spirion also offers additional Premium Support Offerings if customers need more guided and/or direct access to a Support Analyst. The following is a list of Premium Offerings. Please contact your Customer Success Manager to receive more information about these offerings.

Premium Support/ Technical Account Manager (TAM)

- Named and Dedicated Technical Account Manager (TAM)
- Personalized Assistance and Support that knows you and your organization
- Faster Response times
- Shorter time to resolution for configuration issues
- Escalated and Prioritized Support
- Proactive and tailored environmental reviews
- No Support Tickets, TAM handles Support tickets for you
- Low Customer/TAM ratio ensures questions are answered quickly
- Be the first to know about new releases, new features, interesting webinars, and more
- A regular scheduled weekly session with your TAM if desired
- Assistance with all aspects of your Spirion deployment to ensure maximum utilization and maximum ROI
- Direct access to Product Managers
- Direct access to on-staff compliance and legal experts (Assistance limited to 2 hours per year. Additional work to be scoped and charged separately)

Designated Support Analyst

- Support Tickets always route to same Support Engineer
- Personalized Assistance from a Support Engineer who knows your organization
- Bi-Annual Health Check (2) with Professional Services
- Can be combined with Inbound Phone Support

Inbound Phone Support

- US Based Spirion Engineers
- Non-Published, Limited Access, Direct Dial phone support
- Bypass the Support ticket queue and go to the head of the line
- Fast answers to your questions and real-time solutions to your problems
- Can be combined with Designated Support Engineer

Contacting Professional Services

When to contact Professional Services

If assistance is required when configuring or deploying Spirion specifically for your environment, first explore the product documentation and attempt to configure the product without additional assistance. While we do offer Professional Services for a fee, most customers have been able to answer their questions by visiting the Support Portal and [reviewing on-line help](#), [searching KB articles](#), and/or [reading existing documentation](#).

To contact the Professional Services team, please contact your Customer Success Manager. Your Customer Success Manager is the person assigned to manage your account at the time you signed up with Spirion. The purchaser within your organization has the contact information for the appropriate Spirion Customer Success Manager. If you are unable to obtain the proper contact information for your account representative, please contact Support and they will be happy to assist.

The following assistance is not covered by Support but can be covered by Professional Services

- **Configuration Questions** - All of the application settings and configuration scenarios are documented. Questions about the existence of a setting to perform a particular function, details for each specific setting, and the available methods by which to configure settings can be located by searching our [documentation](#) and [KB articles](#). If you require assistance determining the appropriate settings for your requirements or need a review of your settings, please contact Professional Services.
- **Usage Questions** - Training is not generally required on using our applications but, to speed up the learning curve, we do offer professional services to answer questions specific to your environment. Before engaging professional services, please search the [on-line help](#) and let us know if there are ways to improve the documentation and thereby further reduce the need for our customers to acquire training. If you require training on Client or Console applications, please contact Professional Services.
- **Report Writing** - Report Writing is generally not covered by Support but handled by professional services. If you need a custom report please provide a general mockup of what it is you are hoping to achieve with the report when contacting Professional Services.
- **Custom Sensitive Data Definitions (SSD)** - Custom Sensitive Data Definitions can be created with the help of a Professional Services Consultant who understands your use case.
- **Deployment Assistance** - Detailed [documentation](#) exists to create client installers for deployment. If you run into problems, you can follow the documented troubleshooting steps or resolve issues by contacting Windows or Mac administrators or installation/deployment experts within your organization. If you are unable to create a deployment package or need a review of your configuration, please contact Professional Services.

Premium Professional Services Offerings

Classification and Remediation Consulting

- A Spirion Professional Services Engineer and Spirion legal and compliance expert will work with your internal team to develop a classification schema and recommended remediation strategy.
- Spirion's Professional Services Engineer will then work with the organization's Spirion team to configure and implement the classification schema and remediation strategy.

Privacy Risk Profile

- Two Options – On-site or Remote engagement with a Spirion Professional Services Engineer
- All on-prem workstations will be in scope and searched
- Spirion will search up to 450 GB of file server data

- Data volume can be increased for an additional fee

- Data discovery will be limited to Credit Cards, Formatted Social Security Numbers, Passports, Bank Accounts, and Passwords
- The organization will be provided with detailed reports of what data was found, where it was found, the amount of data discovered on the different systems, and more
- Spirion will provide detailed descriptions of scans performed to assist an organization with auditing and compliance
- Typical engagements involve three or four days on-site or remote


Advanced Privacy Risk Assessment

- Two Options – Remote only or hybrid on-site/remote engagement with a Spirion Professional Services Engineer
- For On-Site engagement, A Spirion Professional Services Engineer will be on-site for Kick-off, installation, configuration, and initial test scans
- Spirion Engineer will work with the organization's staff to remotely oversee and manage the searching activities
- All on-prem and VPN connected workstations will be in scope and searched
- Spirion will search up to 7 TB of unstructured data utilizing Discovery Teams
- Data discovery will include Spirion's AnyFinds and custom customer defined search criteria developed with the Spirion Engineer
- The organization will be provided with detailed reports of what data was found, where it was found, the amount of data discovered on the different systems, and more
- Spirion will provide detailed descriptions of scans performed to assist the organization with auditing and compliance
- SoW based engagement



Recent activity

- FAQs
FAQ: Searching MYSQL Connector That Requires TLS 1.2 Article created 9 hours ago 

- Installing, Upgrading, or Deploying
Spinix Installation Check List Article created 10 days ago 

- Troubleshooting
Steps to building a successful connection string for a PostGRES DB Article created 10 days ago 

Attachment C to Purchase Agreement #2021003177

Spirion Software As A Service License Terms

1. SERVICES.

1.1 Access and Use. Subject to the terms and conditions of this Agreement, including, but not limited to, payment by Customer of the applicable fees set forth on Customer issues Purchase Order Spirion grants to Customer a limited, non-exclusive, non-transferable license to remotely access and use the Services that are located on the Spirion Server in accordance with the terms of this Agreement for the length of the Term solely for Customer's internal business purposes. Use of the Services is limited to Authorized Users. Use of the Services is limited to the number of users designated in the Order Form. Customer will establish and maintain, at its own expense, all telecommunications equipment and access lines necessary to gain access to the Services.

1.2 Documentation License. Spirion hereby grants to Customer a non-exclusive, non-sublicensable, non-transferable license to use the Documentation during the Term solely for Customer's internal business purposes in connection with its use of the Services.

1.3 Third-Party Vendors. Spirion acknowledges and agrees that Customer may use certain third-party vendors for purposes of performing some of Customer's internal business processes ("Third-Party Vendors"). Spirion authorizes Customer to allow its Third-Party Vendors (other than Spirion's direct competitors) to access and use the Services subject to the terms and conditions of this Agreement solely for Customer's internal business processing services, subject to the following conditions: (i) Customer agrees to be fully responsible and liable for all use of the Services by its Third-Party Vendors; (ii) Customer will ensure compliance by its Third-Party Vendors of the terms and conditions of this Agreement, including without limitation, Section 4 of this Agreement (Confidential Information); (iii) Customer will formally notify Spirion of any such Third-Party Vendors and will ensure that each such Third-Party Vendor uses its own unique password as detailed in Section 2 below; and (iv) upon termination of its relationship with such Third-Party Vendors or of this Agreement, Customer will ensure that all access to the Services by such Third-Party Vendors ceases immediately.

1.3 Limitations. Unless otherwise expressly authorized in this Agreement, Customer will not, and will ensure that its users will not: (i) modify, adapt, alter, translate, or create Derivative Works from the Documentation (other than providing Spirion with suggestions on improving the Services); (ii) sublicense, resell, re-distribute, lease, rent, loan, disclose or otherwise transfer the Services (or any part thereof), or any other associated products and services, to any third party; (iii) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source or object code of the Services (or any part thereof); (iv) use the Services (or any part thereof) to provide similar services to third parties, or permit third parties to use the Services (or any part thereof) (v) use the Services (or any part thereof) to develop a product line that is similar to the Services or Services or to develop competitive analyses or benchmarking of Spirion's products and services; (vi) otherwise use the Services or copy the Documentation except as expressly allowed under this Agreement; or (vii) alter, distort, or remove any confidential, proprietary, copyright, trademark, trade secret, or patent legends from any copy of the Services (or any part thereof).

1.4 Proprietary Rights. As between the parties, and subject to the terms and conditions of this Agreement, Spirion and its third-party suppliers will retain ownership of all Intellectual Property Rights in the Services, and any and all Derivative Works made to the Services or any part thereof, (“**Spirion Proprietary Technology**”). Customer acquires no rights to Spirion Proprietary Technology except for the licensed interests granted under this Agreement or any SOW. Customer acknowledges and agrees that Spirion may use, without restriction, all suggestions, improvements and ideas concerning any part of the Services or Intellectual Property Rights therein that may be communicated to Spirion by Customer. Customer agrees to inform Spirion immediately of any infringement or other improper action with respect to Spirion’s Confidential Information, the Services or the Intellectual Property Rights therein that comes to Customer’s attention. Customer acknowledges and agrees that Spirion owns all Resultant Data, and may use it for product development purposes.

2. CUSTOMER ACCESS.

2.1 Customer’s Obligations. Spirion will provide Customer with Access Credentials. Customer will ensure that each user is given their own individual user ID and password, which may not be shared with another individual for any reason. Customer is entirely responsible for maintaining the confidentiality of such passwords and of its accounts. Customer is responsible for all access to and use of the Services through Customer's Access Credentials.

2.2 Unauthorized Access. Spirion is not responsible for any unauthorized access and/or use by any third party who independently gains access to Customer Data, provided that such access is not caused or contributed to by Spirion. Spirion will have no liability for any loss or damage arising from Customer’s failure to comply with the provisions of Section 2.1 and 2.2.

3 CUSTOMER DATA AND SECURITY.

3.1 Customer Data Generally. Customer is the sole and exclusive owner of all Customer Data and all Intellectual Property Rights in the Customer Data. Customer Data may include Personally identifiable information (“**PII**”). In the event Customer provides Spirion with PII, the terms of the UC Appendix Data Security and Privacy set forth in Section 14, Incorporated Documents part c) will apply in addition to this Section 3. Customer assumes full responsibility to safeguard against unauthorized access and provide appropriate protection of its Customer Data prior to and during the transmission or transfer of its Customer Data to Spirion

3.2 Customer Information Security Protocols.

Customer has and will retain sole responsibility for: (a) all Customer Data, including permissions to collect, store, process, and transfer Personal Data to Spirion; (b) all information, instructions, and materials provided by or on behalf of Customer or any Authorized User in connection with the Services; (c) Customer Systems; (d) the security and use of Customer’s and its Authorized Users’ Access Credentials; and (e) all access to and use of the Services and Spirion Materials directly or indirectly by or through the Customer Systems or its or its Authorized Users’ Access Credentials, with or without Customer’s knowledge or consent, including all results obtained from, and all conclusions, decisions, and actions based on, such access or use.

3.3 Data Backup. The Services do not replace the need for Customer to maintain regular data backups or redundant data archives. SPIRION HAS NO OBLIGATION OR LIABILITY FOR ANY LOSS,

ALTERATION, DESTRUCTION, DAMAGE, CORRUPTION, OR RECOVERY OF CUSTOMER DATA.

4 PROFESSIONAL SERVICES.

4.1 Professional Services Generally. Spirion will provide Customer any of the following Professional Services: implementation, training, support and maintenance in excess of that provided under Section 6, Support, and transitional services, subject to a Statement of Work, Attachment A to this Purchase Agreement

4.2 Work Product. Any work product of the Professional Services shall remain the property of Spirion, and shall be licensed to Customer at no additional cost for its use exclusively in connection with the Services and for no other purpose.

Attachment D to Purchase Agreement #2021003177

Software License Terms

1. **The Software and Data.** The Parties agree and understand that the Spirion Software is a tool to discover, segregate, and encrypt certain data on Licensee Devices per Licensee's instructions. The Software is to be installed and maintained on-premises on Licensee's computer systems. The Licensee decides which types of Licensee Data it wishes to discover on its devices, for example, credit card numbers. The Software does not transmit Licensee Data to Spirion.

2. **Definitions.**

"Device" means an electronic device owned or leased by Licensee or an Employee which is capable of executing the Software program.

"Defect" means the failure of the Software to substantially conform to the Documentation, when such failure can be reproduced and documented by Spirion.

"Documentation" means product user guides (at URL: www.spirion.com/support/user-guides) relating to the Software that Spirion provides or makes available to Licensee which describe the functionality, components, features, or requirements of the Software, including any aspect of the installation, configuration, integration, operation, or use of the Software.

"Employee" or means an employee or authorized contractor of the Licensee whose job functions require the individual to access or store data on one or more Devices.

"Intellectual Property Rights" means all rights in and to any of the following, however constituted: trade secrets, patents, copyrights, service marks, trademarks, domain names, trade dress, know-how, moral rights, code (executable, object and other) and related and similar rights under the laws of any applicable governmental authority or international treaty, including but not limited to all applications and registrations relating to the foregoing.

License Types:

"Lifetime License" means a license to use the use the current version of the Software and Documentation in perpetuity. The Lifetime License does not include Maintenance or Support, but Licensee may purchase Maintenance and Support on an annual basis.

"Annual License" means a license to use the Software and Documentation for a Term of one year. It includes any Maintenance Releases released during the Term and Support.

"Licensee Data" means any data stored on Devices, not including Usage Data.

"License Quote" means the Spirion document presented to Licensee that lists the Term, fees, licensed Software, and any Maintenance and Support.

"Licensed Product(s)" means the licensed Software and related Documentation.

"Maintenance Release" means any update, upgrade, release, or other adaptation or modification of the Software, including any updated Documentation, that Spirion may make available to Licensee from time to time during the Term, which may contain, among other things, bug fixes, error corrections, enhancements, improvements, or other

changes to the user interface, functionality, compatibility, capabilities, performance, efficiency, or quality of the Software, but does not include any New Version.

“**New Version**” means any new version of the Software that Spirion may from time to time introduce and market generally as a distinct licensed product (as may be indicated by Spirion’s designation of a new version number), and which Spirion may make available to Licensee at an additional cost under a separate written agreement.

“**Permitted Use**” means the use of the Licensed Products by Licensee on its own computer systems for the purpose of discovering sensitive data contained in Licensee Data.

“**Software**” means the executable, object code version of the computer software program(s) identified on a License Quote, and all Maintenance Releases to it made available by Spirion to Licensee during the Term.

“**Supported Platforms**” means the operating systems that Spirion provides Support for.

“**Term**” means the time period of the License as stated on the License Quote or other Addendum.

“**Usage Data**” means records of how Licensee is using the Software.

3. License.

3.1 License Grant. Subject to and conditioned on Licensee’s payment of fees and compliance with all other terms and conditions of this Agreement, Spirion hereby grants to Licensee a non-exclusive, non-transferable, non-sublicensable, worldwide license to use the Licensed Products solely for the Permitted Use during the Term.

3.2 Third Party Licenses. The Licensed Products may include software products licensed from third parties. Such third parties have no obligations or liability to Licensee under this Agreement. Specific third-party license terms applying to portions of the Licensed Products are set forth at the following URL: www.spirion.com/Company/ThirdPartyLicensing and are hereby incorporated by reference.

3.3 License Restrictions. Except as this Agreement expressly permits, Licensee shall not, and shall not permit any other person or entity to:

- (a) copy the Software, in whole or in part;
- (b) modify, correct, adapt, translate, enhance, or otherwise prepare derivative works or improvements of any Software;
- (c) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available the Software to any third party;
- (d) reverse engineer, disassemble, decompile, decode, or adapt the Software, or otherwise attempt to derive or gain access to the source code of the Software, in whole or in part;
- (e) bypass or breach any security device or protection used for or contained in the Software or Documentation;
- (f) remove, delete, efface, alter, obscure, translate, combine, supplement, or otherwise change any trademarks, terms of the Documentation, warranties, disclaimers, or Intellectual Property Rights, proprietary rights or other symbols, notices, marks, or serial numbers on or relating to any copy of the Software or Documentation;
- (g) use the Software in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Right or other right of any person or entity, or that violates any applicable Law;

(h) use the Software for purposes of: (i) benchmarking or competitive analysis of the Software; (ii) developing, using, or providing a competing software product or service; or (iii) any other purpose that is to Spirion's detriment or commercial disadvantage; or

(i) use the Software in or in connection with the design, construction, maintenance, operation, or use of any hazardous environments, systems, or applications, any safety response systems or other safety-critical applications, or any other use or application in which the use or failure of the Software could lead to personal injury or severe physical or property damage.

3.4 Licensee may use the Software to search the data only on the Devices of the number of Employees authorized by this Agreement. If an Employee leaves the employment of or engagement with the Licensee, Licensee may reallocate the use of the Software to include another Employee.

4 License Compliance Measures; Audit Rights and Remedies.

4.1 The Software may contain technological copy protection or other security features designed to prevent unauthorized use of the Software. Licensee shall not, and shall not attempt to, remove, disable, circumvent or otherwise create or implement any workaround to, any such copy protection

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

1.0 -Scope of National Cooperative Contract

Capitalized terms not otherwise defined herein shall have the meanings given to them in the Master Agreement or in the Administration Agreement between Supplier and OMNIA Partners.

1.1 Requirement

The University of California (hereinafter defined and referred to as “Principal Procurement Agency”), on behalf of itself and the National Intergovernmental Purchasing Alliance Company, a Delaware corporation d/b/a OMNIA Partners, Public Sector (“**OMNIA Partners**”), is requesting proposals for IT Security Tools. The intent of this Request for Proposal is any contract between Principal Procurement Agency and Supplier resulting from this Request for Proposal (“**Master Agreement**”) be made 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. The Principal Procurement Agency has executed a Principal Procurement Agency Certificate with OMNIA Partners, an example of which is included as Exhibit D, and has agreed to pursue the Master Agreement. Use of the Master Agreement by any Public Agency is preceded by their registration with OMNIA Partners as a Participating Public Agency in OMNIA Partners’ cooperative purchasing program. Registration with OMNIA Partners as a Participating Public Agency is accomplished by Public Agencies entering into a Master Intergovernmental Cooperative Purchasing Agreement, an example of which is attached as Exhibit C, and by using the Master Agreement, any such Participating Public Agency agrees that it is registered with OMNIA Partners, whether pursuant to the terms of the Master Intergovernmental Purchasing Cooperative Agreement or as otherwise agreed to. The terms and pricing established in the resulting Master Agreement between the Supplier and the Principal Procurement Agency will be the same as that available to Participating Public Agencies through OMNIA Partners.

All transactions, purchase orders, invoices, payments etc., will occur directly between the Supplier and each Participating Public Agency individually, and neither OMNIA Partners, any Principal Procurement Agency nor any Participating Public Agency, including their respective agents, directors, employees or representatives, shall be liable to Supplier for any acts, liabilities, damages, etc., incurred by any other Participating Public Agency. Supplier is responsible for knowing the tax laws in each state.

This Exhibit A defines the expectations for qualifying Suppliers based on OMNIA Partners’ requirements to market the resulting Master Agreement nationally to Public Agencies. Each section in this Exhibit A refers to the capabilities, requirements, obligations, and prohibitions of competing Suppliers on a national level in order to serve Participating Public Agencies through OMNIA Partners.

These requirements are incorporated into and are considered an integral part of this RFP. OMNIA Partners reserves the right to determine whether or not to make the Master Agreement awarded by the Principal Procurement Agency available to Participating Public Agencies, in its sole and absolute discretion, and any party submitting a response to this RFP acknowledges that any award

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

by the Principal Procurement Agency does not obligate OMNIA Partners to make the Master Agreement available to Participating Procurement Agencies.

1.2 Marketing , Sales and Administrative Support

During the term of the Master Agreement OMNIA Partners intends to provide marketing, sales, partnership development and administrative support for Supplier pursuant to this section that directly promotes the Supplier's products and services to Participating Public Agencies through multiple channels, each designed to promote specific products and services to Public Agencies on a national basis.

OMNIA Partners will assign the Supplier a Director of Partner Development who will serve as the main point of contact for the Supplier and will be responsible for managing the overall relationship between the Supplier and OMNIA Partners. The Director of Partner Development will work with the Supplier to develop a comprehensive strategy to promote the Master Agreement and will connect the Supplier with appropriate stakeholders within OMNIA Partners including, Sales, Marketing, Contracting, Training, Operations & Support.

The OMNIA Partners marketing team will work in conjunction with Supplier to promote the Master Agreement to both existing Participating Public Agencies and prospective Public Agencies through channels that may include:

- A. Marketing collateral (print, electronic, email, presentations)
- B. Website
- C. Trade shows/conferences/meetings
- D. Advertising
- E. Social Media

The OMNIA Partners sales teams will work in conjunction with Supplier to promote the Master Agreement to both existing Participating Public Agencies and prospective Public Agencies through initiatives that may include:

- A. Individual sales calls
- B. Joint sales calls
- C. Communications/customer service
- D. Training sessions for Public Agency teams
- E. Training sessions for Supplier teams

The OMNIA Partners contracting teams will work in conjunction with Supplier to promote the Master Agreement to both existing Participating Public Agencies and prospective Public Agencies through:

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

- A. Serving as the subject matter expert for questions regarding joint powers authority and state statutes and regulations for cooperative purchasing
- B. Training sessions for Public Agency teams
- C. Training sessions for Supplier teams
- D. Regular business reviews to monitor program success
- E. General contract administration

1.3 Estimated Volume

The dollar volume purchased under the Master Agreement is estimated to be approximately__ million annually. While no minimum volume is guaranteed to Supplier, the estimated annual volume is projected based on the current annual volumes among the Principal Procurement Agency, other Participating Public Agencies that are anticipated to utilize the resulting Master Agreement to be made available to them through OMNIA Partners, and volume growth into other Public Agencies through a coordinated marketing approach between Supplier and OMNIA Partners.

1.4 Award Basis

The basis of any contract award resulting from this RFP made by Principal Procurement Agency will, at OMNIA Partners option, be the basis of award on a national level through OMNIA Partners. If multiple Suppliers are awarded by Principal Procurement Agency under the Master Agreement, those same Suppliers will be required to extend the Master Agreement to Participating Public Agencies through OMNIA Partners. Utilization of the Master Agreement by Participating Public Agencies will be at the discretion of the individual Participating Public Agency. Certain terms of the Master Agreement specifically applicable to the Principal Procurement Agency (e.g. governing law) are subject to modification for each Participating Public Agency as Supplier, such Participating Public Agency and OMNIA Partners shall agree without being in conflict with the Master Agreement. Participating Agencies may request to enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in the Master Agreement (i.e. invoice requirements, order requirements, specialized delivery, diversity requirements such as minority and woman owned businesses, historically underutilized business, governing law, etc.). It shall be the responsibility of the Supplier to comply, when applicable, with the prevailing wage legislation in effect in the jurisdiction of the Participating Agency. It shall further be the responsibility of the Supplier to monitor the prevailing wage rates as established by the appropriate department of labor for any increase in rates during the term of the Master Agreement and adjust wage rates accordingly. Any supplemental agreement developed as a result of the Master Agreement is exclusively between the Participating Agency and the Supplier (Contract Sales are reported to OMNIA Partners).

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

All purchase orders issued and accepted by the Supplier may survive expiration or termination of the Master Agreement. Participating Agencies' purchase orders may exceed the term of the Master Agreement if the purchase order is issued prior to the expiration of the Master Agreement. Supplier is responsible for reporting all sales and paying the applicable administrative fee for sales that use the Master Agreement as the basis for the purchase order, even though Master Agreement may have expired.

1.5 Objectives of Cooperative Program

This RFP is intended to achieve the following objectives regarding availability through OMNIA Partners' cooperative program:

- A. Provide a comprehensive competitively solicited and awarded national agreement offering the Products covered by this solicitation to Participating Public Agencies;
- B. Establish the Master Agreement as the Supplier's primary go to market strategy to Public Agencies nationwide;
- C. Achieve cost savings for Supplier and Public Agencies through a single solicitation process that will reduce the Supplier's need to respond to multiple solicitations and Public Agencies need to conduct their own solicitation process;
- D. Combine the aggregate purchasing volumes of Participating Public Agencies to achieve cost effective pricing.

2.0 REPRESENTATIONS AND COVENANTS

As a condition to Supplier entering into the Master Agreement, which would be available to all Public Agencies, Supplier must make certain representations, warranties and covenants to both the Principal Procurement Agency and OMNIA Partners designed to ensure the success of the Master Agreement for all Participating Public Agencies as well as the Supplier.

2.1 Corporate Commitment

Supplier commits that (1) the Master Agreement has received all necessary corporate authorizations and support of the Supplier's executive management, (2) the Master Agreement is Supplier's primary "go to market" strategy for Public Agencies, (3) the Master Agreement will be promoted to all Public Agencies, including any existing customers, and Supplier will transition existing customers, upon their request, to the Master Agreement, and (4) that the Supplier has read and agrees to the terms and conditions of the Administration Agreement with OMNIA Partners and will execute such agreement concurrent with and as a condition of its execution of the Master Agreement with the Principal Procurement Agency. Supplier will identify an executive corporate sponsor and a separate national account manager within the RFP response that will be responsible for the overall management of the Master Agreement.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

2.2 Pricing Commitment

Supplier commits the not-to-exceed pricing provided under the Master Agreement pricing is its lowest available (net to buyer) to Public Agencies nationwide and further commits that if a Participating Public Agency is eligible for lower pricing through a national, state, regional or local or cooperative contract, the Supplier will match such lower pricing to that Participating Public Agency under the Master Agreement.

2.3 Sales Commitment

Supplier commits to aggressively market the Master Agreement as its go to market strategy in this defined sector and that its sales force will be trained, engaged and committed to offering the Master Agreement to Public Agencies through OMNIA Partners nationwide. Supplier commits that all Master Agreement sales will be accurately and timely reported to OMNIA Partners in accordance with the OMNIA Partners Administration Agreement. Supplier also commits its sales force will be compensated, including sales incentives, for sales to Public Agencies under the Master Agreement in a consistent or better manner compared to sales to Public Agencies if the Supplier were not awarded the Master Agreement.

3.0 SUPPLIER RESPONSE

Supplier must supply the following information in order for the Principal Procurement Agency to determine Supplier's qualifications to extend the resulting Master Agreement to Participating Public Agencies through OMNIA Partners.

3.1 Company

- A. Brief history and description of Supplier.
 - i. Following is a link to our most current information regarding Spirion and our solutions. <https://www.spirion.com/company/>
- B. Total number and location of sales persons employed by Supplier.
 - i. We have approximately 120 employees.
 - ii. Corporate headquarters is located in St Petersburg, FL
- C. Number and location of support centers (if applicable) and location of corporate office.
 - i. Support center is located at the corporate headquarters in St Petersburg, FL
- D. Annual sales for the three previous fiscal years.
 - i. Spirion is a privately held LLC by Riverside Company (riversidecompany.com). The Riverside Company is a growth equity firm with over \$9 billion in assets under management. Spirion has been incorporated since 2001 and is an industry leader in the data discovery and automated classification space.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

E. Submit FEIN and Dunn & Bradstreet report.

- i. FEIN 13-4183707
- ii. Dunn # 80-121-3609

F. Describe any green or environmental initiatives or policies.

- i. Policies are updated regularly. As a software solution we maintain a small footprint.

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.

- i. Spirion believes in helping clients manage data security and compliance initiatives together with partners. We are the leader in data discovery, classification, and privacy for organizations of all types and sizes, helping to transform the biggest threat to an organization's security: the mass proliferation of sensitive data. Our company has enjoyed exponential growth year over year and partnership with us can help prospective partners unlock new revenue streams

H. Describe any historically underutilized business certifications supplier holds and the certifying agency. This may include business enterprises such as minority and women owned, small or disadvantaged, disable veterans, etc.

- i. n/a

I. Describe how supplier differentiates itself from its competitors.

- i. Spirion's approach to data discovery includes our patented Privacy Grade technology. Additional details are included with the RFP response.
- ii. The Spirion platform accurately discovers structured and unstructured sensitive data across campuses — from the network to the cloud — including students' personally identifiable data (PII), protected health information (PHI), and credit card numbers. It classifies data according to compliance regulations and campus rules. And it integrates with schools' preferred security apps to lock down data protection.
- iii. Spirion empowers higher education institutions with full data visibility, so they can determine strategic protections and actions, and monitor progress without burdening their IT staff or risking human error. This fortifies sensitive data protection — and ensures that data is given the right protections, while providing the flexibility that allows admins to perform critical data-centric operations.

J. Describe any present or past litigation, bankruptcy or reorganization involving supplier.

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

i. n/a

K. Felony Conviction Notice: Indicate if the supplier

i. n/a

b. is a publicly held corporation and this reporting requirement is not applicable;

c. is not owned or operated by anyone who has been convicted of a felony; or

d. is owned or operated by and individual(s) who has been convicted of a felony and provide the names and convictions.

L. Describe any debarment or suspension actions taken against supplier

i. n/a

3.2 Distribution, Logistics

A. Describe the full line of products and services offered by supplier.

i. Here is a link that provides current product and services information <https://www.spirion.com/products/data-privacy-manager/>

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.

i. Software is delivered electronically, and services are provided remotely.

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.

i. All entities that fall into the category of SLED businesses run through the Spirion SLED team who monitors for appropriate contract uses and pricing. It is that team who will ensure the best possible pricing is applied based on contract eligibility.

D. Identify all other companies that will be involved in processing, handling or shipping the products/service to the end user.

i. n/a

E. Provide the number, size and location of Supplier's distribution facilities, warehouses and retail network as applicable.

i. n/a

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

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

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
- iii. 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:
 - iv. Creation and distribution of a co-branded press release to trade publications
 - v. Announcement, Master Agreement details and contact information published on the Supplier's website within first 90 days
 - vi. Design, publication and distribution of co-branded marketing materials within first 90 days
 - vii. Commitment to attendance and participation with OMNIA Partners 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
 - viii. Commitment to attend, exhibit and participate at the NIGP Annual Forum in an area reserved by OMNIA Partners 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.
 - ix. Design and publication of national and regional advertising in trade publications throughout the term of the Master Agreement
 - x. Ongoing marketing and promotion of the Master Agreement throughout its term (case studies, collateral pieces, presentations, promotions, etc.)
 - xi. Dedicated OMNIA Partners internet web-based homepage on Supplier's website with:
 - OMNIA Partners 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' website including the online registration page;

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

Spirion will work with our marketing and executive team to ensure we provide a sales process and motion that best leverages the new relationship enabling us to work together and provide a Privacy Grade solution.

In today's ever-changing higher education institutions, it's difficult to know where sensitive student and staff data resides. This makes it even more difficult to take the right security precautions necessary to protect their data — which creates high risk for universities and colleges. Spirion delivers a platform that executes data compliance and security smarter.

From HIPAA to PCI, higher education institutions must comply with multiple data security regulations to protect an ever-expanding body of student and staff sensitive data. A Spirion-first approach makes it easy to proactively protect their sensitive data with persistent data discovery, classification, and protection.

B. Describe how Supplier will transition any existing Public Agency customers' accounts to the Master Agreement available nationally through OMNIA Partners. Include a list of current cooperative contracts (regional and national) Supplier holds and describe how the Master Agreement will be positioned among the other cooperative agreements.

- i. Our SLED team will review all pending opportunities to ensure we are able to leverage the OMNIA partners purchasing vehicle including current maintenance and subscription clients.

C. 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.

- i. Acknowledged

D. 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. All sales materials are to use the OMNIA Partners 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
 - a. Confirmed

E. 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

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

- iii. Awareness of the range of Public Agencies that can utilize the Master Agreement through OMNIA Partners
- iv. Knowledge of benefits of the use of cooperative contracts
 - a. Confirmed

F. Provide the name, title, email and phone number for the person(s), who will be responsible for:

- i. Executive Support
- ii. Marketing
- iii. Sales
- iv. Sales Support
- v. Financial Reporting
- vi. Accounts Payable
- vii. Contracts

- i. Initially all communication will go through the SLED POD Lead. A dedicated email alias will be created to allow for easy capture of communication.
- ii. Marla Santino
- iii. Marla.santino@spirion.com
- iv. (503)522-5453

G. 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.

- i. The SLED team has a leader who covers Enterprise level accounts. Additionally, there are mid-market representatives, Customer success managers for post sales activities.

H. Explain in detail how the sales teams will work with the OMNIA Partners team to implement, grow and service the national program.

- i. In conjunction with our channel and marketing team, Spirion will work closely to align opportunities with our Omnia partners.

I. 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.

- i. team will be assigned to help develop and monitor the ongoing effort of the agreement.

J.

- i. As a privately held company this information is not public however we can provide references upon approval to proceed to the next step of

OMNIA PARTNERS EXHIBITS
EXHIBIT A- RESPONSE FOR NATIONAL COOPERATIVE CONTRACT

the award process. References are being provided as part of the RFP associated with this agreement.

K. 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.

- i. Spirion has the systems in place to receive and process orders as needed for this agreement

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.

Spirion is open to review and discuss the minimum dollar transaction through the agreement once approved to proceed to the next step in the process.

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.

We will review each of these options when faced with a solicitation outside of this agreement including a reference back to this partnership with OMNIA.

SOFTWARE AS A SERVICE AGREEMENT

TERM AND CONDITIONS

These terms and conditions (“Terms and Conditions”) govern all orders signed by Customer (each an “Order”) for use of Spirion’s Services (as defined in the Definitions). Each Order and these Terms and Conditions together constitute the Software as a Service Agreement (“**Agreement**”) between Spirion, LLC, a Delaware limited liability company with offices located at 200 Central Ave., Suite 1900, St. Petersburg, FL 33701 (“**Spirion**”) and the customer identified on the Order Form (“**Customer**”). The **Effective Date** of this Agreement is the date specified on the Order Form.

Schedule A: Definitions

Schedule B: Initial Order Form

Schedule C: Customer Support Services and SLAs

Schedule D: Data Protection Addendum

Schedule E: Professional Services SOW

The parties hereby cause this Agreement to be executed by their respective duly authorized representatives effective as of the Effective Date.

Accepted and Agreed:

[Customer's Legal Entity]

By: _____

Name: _____

Title: _____

Date: _____

Address: _____

Telephone: _____

Email: _____

Spirion, LLC

By: _____

Name: _____

Title: _____

Date: _____

Address: _____

Telephone: _____

Email: _____

1. SERVICES.

1.1 Access and Use. Subject to the terms and conditions of this Agreement, including, but not limited to, payment by Customer of the applicable fees set forth on the Order Form, Spirion grants to Customer a limited, non-exclusive, non-transferable (except as permitted under Section 13.4 of the Terms and Conditions) license to remotely access and use the Services that are located on the Spirion Server in accordance with the terms of this Agreement for the length of the Term solely for Customer's internal business purposes. Use of the Services is limited to Authorized Users. Use of the Services is limited to the number of users designated in the Order Form. Customer will establish and maintain, at its own expense, all telecommunications equipment and access lines necessary to gain access to the Services.

1.2 Documentation License. Spirion hereby grants to Customer a non-exclusive, non-sublicensable, non-transferable (except as permitted under Section 13.4 of the Terms and Conditions) license to use the Documentation during the Term solely for Customer's internal business purposes in connection with its use of the Services.

1.3 Third-Party Vendors. Spirion acknowledges and agrees that Customer may use certain third-party vendors for purposes of performing some of Customer's internal business processes ("**Third-Party Vendors**"). Spirion authorizes Customer to allow its Third-Party Vendors (other than Spirion's direct competitors) to access and use the Services subject to the terms and conditions of this Agreement solely for Customer's internal business processing services, subject to the following conditions: (i) Customer agrees to be fully responsible and liable for all use of the Services by its Third-Party Vendors; (ii) Customer will ensure compliance by its Third-Party Vendors of the terms and conditions of this Agreement, including without limitation, Section 4 of this Agreement (Confidential Information); (iii) Customer will formally notify Spirion of any such Third-Party Vendors and will ensure that each such Third-Party Vendor uses its own unique password as detailed in Section 2 below; and (iv) upon termination of its relationship with such Third-Party Vendors or of this Agreement, Customer will ensure

that all access to the Services by such Third-Party Vendors ceases immediately.

1.3 Limitations. Unless otherwise expressly authorized in this Agreement, Customer will not, and will ensure that its users will not: (i) modify, adapt, alter, translate, or create Derivative Works from the Documentation (other than providing Spirion with suggestions on improving the Services); (ii) sublicense, resell, re-distribute, lease, rent, loan, disclose or otherwise transfer the Services (or any part thereof), or any other associated products and services, to any third party; (iii) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source or object code of the Services (or any part thereof); (iv) use the Services (or any part thereof) to provide similar services to third parties, or permit third parties to use the Services (or any part thereof) (v) use the Services (or any part thereof) to develop a product line that is similar to the Services or Services or to develop competitive analyses or benchmarking of Spirion's products and services; (vi) otherwise use the Services or copy the Documentation except as expressly allowed under this Agreement; or (vii) alter, distort, or remove any confidential, proprietary, copyright, trademark, trade secret, or patent legends from any copy of the Services (or any part thereof).

1.4 Proprietary Rights. As between the parties, and subject to the terms and conditions of this Agreement, Spirion and its third-party suppliers will retain ownership of all Intellectual Property Rights in the Services, and any and all Derivative Works made to the Services or any part thereof, ("**Spirion Proprietary Technology**"). Customer acquires no rights to Spirion Proprietary Technology except for the licensed interests granted under this Agreement or any SOW. Customer acknowledges and agrees that Spirion may use, without restriction, all suggestions, improvements and ideas concerning any part of the Services or Intellectual Property Rights therein that may be communicated to Spirion by Customer. Customer agrees to inform Spirion immediately of any infringement or other improper action with respect to Spirion's Confidential Information, the Services or the Intellectual Property Rights therein that comes to Customer's attention.

Customer acknowledges and agrees that Spirion owns all Resultant Data, and may use it for product development purposes.

1.5 Rights Reserved. Except as set forth in this Agreement, no right or implied license, or right of any kind, is granted to Customer or to any other person or entity with regard to the Services or any part thereof. Nothing in this Agreement confers upon either party any right to use the other party's trade names and trademarks, except for the permitted license use in accordance with this Agreement. All use of such marks by either party will inure to the benefit of the owner of such marks, the use of which will be subject to specifications controlled by the owner.

2. CUSTOMER ACCESS.

2.1 Customer's Obligations. Spirion will provide Customer with Access Credentials. Customer will ensure that each user is given their own individual user ID and password, which may not be shared with another individual for any reason. Customer is entirely responsible for maintaining the confidentiality of such passwords and of its accounts. Customer is responsible for all access to and use of the Services through Customer's Access Credentials.

2.2 Unauthorized Access. Spirion is not responsible for any unauthorized access and/or use by any third party who independently gains access to Customer Data, provided that such access is not caused or contributed to by Spirion. Customer will notify Spirion promptly of any unauthorized use of any user accounts or of any other breach of security occurring as a result of any activities of any of Customer's users or of any vulnerabilities that Customer believes are contained in or caused by the Services such that Spirion may take or recommend appropriate remedial measures. Spirion will have no liability for any loss or damage arising from Customer's failure to comply with the provisions of Section 2.1 and 2.2.

3. FEES AND PAYMENT TERMS.

3.1 Payments. Customer will pay to Spirion all fees due to Spirion under this Agreement in U.S. dollars (collectively "**Fees**"). Unless otherwise set forth in this Agreement, all Fees will be due within thirty (30) days after the date of the invoice for same. All Fees

payable under this Agreement are fully earned, non-cancelable and the sums paid are non-refundable. If any amounts are withheld by Customer in good faith, Customer will, within fifteen (15) days from receipt of invoice ("**Dispute Period**"), provide Spirion a reasonably detailed written explanation of the nature of the dispute, which explanation will set forth the dollar amounts withheld and the reasons for withholding such amounts. If Customer does not dispute the applicable invoice during the Dispute Period, any such dispute will be deemed waived. For clarity, Customer remains obligated to pay Spirion for all portions of the applicable invoice that are not under reasonable and good faith dispute.

3.2 Excess Usage. If, during any thirty (30) day period, Customer uses in excess of the processing agents or storage listed in the Order Form, Spirion shall notify Customer that its use is exceeding the such amount(s). After such notice, Spirion has the right to cap and limit the usage or charge for such overage for the remainder of the Term.

3.3 Overdue Accounts. A late fee may be charged by Spirion on all undisputed Fees and Expenses not paid to Spirion by Customer within thirty (30) days after receipt of the invoice for same at the lesser of the maximum amount chargeable by law or one and one-half percent (1½%) per month commencing with the date payment was due. Customer will be liable for all costs of collection of such undisputed, overdue amounts including, without limitation, all court costs and attorneys' fees incurred by Spirion. Fees due from Customer under this Agreement may not be withheld or offset by Customer against other amounts for any reason.

3.4 Taxes. The Fees and other charges do not include any applicable sales, use, and other taxes (including value added tax) and all applicable export and import fees, customs duties and similar charges, and Customer will also be responsible for the payment of all such taxes (other than taxes based on Spirion's income), fees, duties, and charges, and any related penalties and interest, which will be above and beyond, and in addition to, the Fees, arising from the payment of the Fees and from the delivery of the Services to Customer, whether such taxes are assessed before or retroactively following the issue of any invoice by Spirion. If Customer is required

by law to deduct or withhold any tax or other amount from any sum payable to Spirion, then the sum payable by Customer will be increased to the extent necessary to ensure that after such tax or other amount has been deducted, withheld or paid, Spirion receives on the due date and retains (free from any liability in respect of any such deduction, withholding or payment) a net sum equal to what it would have received and so retained had no such deduction, withholding or payment been required or made.

4. CONFIDENTIAL INFORMATION.

4.1 Disclosure of Confidential Information.

Neither party may use or disclose any Confidential Information of the other party, except on a need-to-know basis for purposes of performing its obligations under this Agreement. This Agreement and its terms are Confidential Information. Disclosure of Confidential Information to employees of the parties hereto will be limited to those who have a need to know such information in connection with carrying out the obligations of the applicable party pursuant to this Agreement. Customer acknowledges that all parts of the Services are the Confidential Information of Spirion and/or Spirion's licensors, and Customer agrees to treat such information as Confidential Information in accordance with the terms of this Agreement. A "party" (as used in this Section 6) will be deemed to include each party's respective subsidiaries, affiliates and sister companies or any other organization in which such party has an ownership stake or over which such party can exert control, and each such party will cause its parties observe the confidentiality requirements of this Agreement with respect to the information disclosed by the other party under this Agreement. The receiving party will only allow its independent contractors to receive the Confidential Information if such contractors execute nondisclosure agreements with, or are otherwise contractually bound to, Confidential Information restrictions no less protective than those of this Agreement; provided that the receiving party will not under any circumstances provide access to such Confidential Information to competitors of Spirion.

4.2 Legally Required Disclosures. If a receiving party is presented with legal process under which it

could be legally compelled to disclose any Confidential Information of the disclosing party (whether by oral question, deposition, interrogatory, request for documents, subpoena, civil investigative demand or similar process or by rule, regulation or other applicable law), such receiving party will promptly notify the disclosing party of the same before any disclosure is made so that the disclosing party may, at its discretion, seek a protective order or other appropriate remedy or may waive compliance with the confidentiality terms of this Agreement. If such protective order or other remedy is not obtained, or if the disclosing party waives compliance with the provisions hereof, then only that portion of the Confidential Information that it is legally required to be disclosed (as advised by a written opinion of counsel) may be disclosed.

4.3 Exclusions to Confidential Information. For purposes of this Agreement, "Confidential Information" will not include information or material which (a) enters the public domain (other than as a result of a breach of this Agreement); (b) was in the receiving party's possession prior to its receipt from the disclosing party; (c) is independently developed by the receiving party without the use of Confidential Information; or (d) is obtained by the receiving party from a third party under no obligation of confidentiality to the disclosing party. Section 7 of this Agreement and any business associate agreement Customer requires Spirion to execute will govern all use and protection of Customer Data.

4.4 Duration and Injunctive Relief. The confidentiality obligations set forth in this Section 4 will continue indefinitely following termination or expiration of this Agreement for as long as the Confidential Information remains a trade secret under applicable law and will continue for three (3) years following termination or expiration of this Agreement with respect to Confidential Information that does not rise to the level of a trade secret. The receiving party acknowledges that disclosure of any Confidential Information or a trade secret by it or its employees will give rise to irreparable injury to the disclosing party or the owner of such information and that such injury will not adequately be compensated for by damages. Accordingly, the disclosing party will be entitled to seek equitable relief, including injunctive relief and specific performance against the

breach or threatened breach of the undertakings in this Section 4, in addition to any other legal remedies which may be available.

5. CUSTOMER DATA AND SECURITY.

5.1 Customer Data Generally. Customer is the sole and exclusive owner of all Customer Data and all Intellectual Property Rights in the Customer Data. Customer Data may include Personally identifiable information (“PII”). In the event Customer provides Spirion with PII, the terms of the Data Protection Addendum set forth in Schedule D will apply in addition to this Section 5. Customer assumes full responsibility to safeguard against unauthorized access and provide appropriate protection of its Customer Data prior to and during the transmission or transfer of its Customer Data to Spirion.

5.2 Spirion Information Security Protocols. Spirion will employ security measures in accordance with Schedule D.

5.3 Customer Information Security Protocols.

Customer has and will retain sole responsibility for: (a) all Customer Data, including permissions to collect, store, process, and transfer Personal Data to Spirion; (b) all information, instructions, and materials provided by or on behalf of Customer or any Authorized User in connection with the Services; (c) Customer Systems; (d) the security and use of Customer’s and its Authorized Users’ Access Credentials; and (e) all access to and use of the Services and Spirion Materials directly or indirectly by or through the Customer Systems or its or its Authorized Users’ Access Credentials, with or without Customer’s knowledge or consent, including all results obtained from, and all conclusions, decisions, and actions based on, such access or use.

Customer shall employ all physical, administrative, and technical controls, screening, and security procedures and other safeguards necessary to: (a) securely administer the distribution and use of all Access Credentials and protect against any unauthorized access to or use of the Services; and (b) control the content and use of Customer Data, including the uploading or other provision of Customer Data for Processing by the Services.

5.3 Data Backup. The Services do not replace the need for Customer to maintain regular data backups or

redundant data archives. SPIRION HAS NO OBLIGATION OR LIABILITY FOR ANY LOSS, ALTERATION, DESTRUCTION, DAMAGE, CORRUPTION, OR RECOVERY OF CUSTOMER DATA.

6. PROFESSIONAL SERVICES.

6.1 Professional Services Generally. Spirion will provide Customer any of the following Professional Services: implementation, training, support and maintenance in excess of that provided under Schedule C, and transitional services, subject to a Statement of Work (“SOW”) (Schedule E).

6.2 Statements of Work. Each SOW shall be incorporated into and subject to this Agreement.

6.3 Work Product. Any work product of the Professional Services shall remain the property of Spirion, and shall be licensed to Customer for its use exclusively in connection with the Services and for no other purpose.

7. CUSTOMER SUPPORT SERVICES AND SLAs.

7.1 Customer Support Services. Spirion will provide the Customer Support Services set forth in Schedule C. Spirion may update this Schedule from time to time upon notice to Customer by providing at least six months of prior written notice. Customer’s continued use of the Services following notice of such changes will constitute Customer’s acceptance of the same.

7.2 SLAs. Spirion will provide the Services in accordance with the service levels set forth in Schedule C.

8. WARRANTY AND DISCLAIMER.

8.1 General Warranty. Each party represents and warrants that it is not subject to any agreement that would prevent it from complying with this Agreement. Spirion represents and warrants that it will comply with all applicable laws and regulations relating to its performance of the Services under this Agreement.

8.2 Professional Services Warranty. Spirion warrants that the Professional Services will be performed in a professional and workmanlike manner consistent with generally accepted industry

practices. For any breach of this services warranty, Customer's exclusive remedy and Spirion's entire liability will be the re-performance of any such deficient Spirion Professional Services. In order to claim a breach of this Professional Services warranty, Customer must identify in a written notice to Spirion any deficiencies in such Professional Services within ninety (90) days of the completion of such deficient Professional Services in order to receive the above warranty remedies.

8.3 Customer Warranty. Customer represents and warrants that Customer is authorized to provide Spirion with the Customer Data, and that Spirion is authorized to use such Customer Data solely for the purpose of providing the Services. Customer also represents and warrants that it will (a) maintain and update an industry standard anti-virus program within its own computer systems and (b) to use commercially reasonable efforts require its employees to check attachments to e-mail messages that its employees receive before saving such attachments to Customer's hard drives or servers.

8.4 DISCLAIMER. OTHER THAN AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER SPIRION, ITS AFFILIATES, LICENSORS OR SUPPLIERS, NOR THEIR OFFICERS, DIRECTORS, EMPLOYEES, SHAREHOLDERS, AGENTS OR REPRESENTATIVES MAKES ANY EXPRESS OR IMPLIED WARRANTIES, CONDITIONS, OR REPRESENTATIONS TO CUSTOMER, OR ANY OTHER PERSON OR ENTITY WITH RESPECT TO THE SOFTWARE, SYSTEM AND SPIRION SERVICES PROVIDED HEREUNDER OR OTHERWISE REGARDING THIS AGREEMENT, WHETHER ORAL OR WRITTEN, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, THE IMPLIED WARRANTY AGAINST INFRINGEMENT, AND THE IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE. SPIRION DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE, SYSTEM OR SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. THE SERVICES USE SEARCH ALGORITHMS TO IDENTIFY SENSITIVE DATA

WITHIN THE CUSTOMER DATA, BUT ARE NOT GUARANTEED TO FIND EVERY OCCURRENCE OF SENSITIVE DATA. CUSTOMER ACKNOWLEDGES THAT USING THE SERVICES, EVEN AS DIRECTED, DOES NOT GUARANTEE COMPLIANCE WITH ANY PARTICULAR LAW, REGULATION, STANDARD, OR BEST PRACTICE, EACH OF WHICH SPIRION EXPRESSLY DISCLAIMS TO THE FULLEST EXTENT OF THE LAW. SPIRION SHALL NOT BE LIABLE UNDER ANY THEORY FOR CUSTOMER'S VIOLATION OR BREACH OF ANY LAW, REGULATION OR STANDARD, EVEN IF SUCH VIOLATION OR BREACH INVOLVED CUSTOMER'S USE OF THE SPIRION SERVICES.

9. INDEMNIFICATION.

9.1 Spirion Indemnity. Spirion will indemnify, defend, and hold Customer, its individual directors, officers, employees and agents, harmless from and against any claims, actions or proceedings, arising out of any third-party claim that the Services or Customer's permitted use thereof infringes or violates any third party's valid U.S. patent, copyright or trade secret ("**IP Claim**"). If in Spirion's reasonable judgment any such IP Claims, or threat of an IP Claim, materially interferes with Customer's use of the Services, Spirion will consult with Customer, and Spirion will have the option, in Spirion's sole discretion, to (a) substitute functionally equivalent non-infringing services or documentation, (b) modify the Services to make it non-infringing, or (c) obtain for Customer at Spirion's expense the right to continue using the infringing Services; or, if the foregoing is not feasible in Spirion's sole discretion, Spirion will (d) require Customer to cease using the Services, refund a pro-rata portion of the Fees (as defined in the Order Form at Schedule B) for the Services for such period of time in which Customer was unable to use the Services. Spirion will have no indemnity obligation for claims of infringement resulting or alleged to result from (i) any combination, operation, or use of any software with any programs or equipment not supplied by Spirion or not specified in this Agreement for such purpose if in Spirion's reasonable judgment such infringement would have been avoided by the combination, operation, or use of such software with

items supplied by Spirion or specified in this Agreement for such purpose; (ii) inclusion of Customer Data; (iii) any modification of the Services by a party other than Spirion if such infringement would have been avoided in the absence of such modifications; or (iv) the use of the Services in a manner other than for its intended purposes or contrary to the Specifications. This Section 9.1 states Spirion's entire liability and Customer's sole and exclusive remedy for infringement claims and actions.

9.2 Customer Indemnity. Customer will indemnify, defend, and hold Spirion, its individual directors, officers, employees, representatives, and agents, harmless from and against any claims, actions or proceedings, arising out of any third-party claim: (a) resulting from Customer's improper use of the Services; or (b) that the Customer Data or Customer's transmission to Spirion or Spirion's hosting or Processing thereof infringes or violates the rights of such third party or violates applicable law.

9.3 General. The defense and indemnification obligations set forth in this Section 9 are conditioned upon (i) the indemnified party providing the indemnifying party timely notice of any claim or cause of action upon which the indemnified party intends to base a claim of indemnification hereunder, (ii) the indemnified party providing reasonable assistance and cooperation to enable the indemnifying party to defend the action or claim hereunder; and (iii) allowing the indemnifying party to control the defense and all related settlement negotiations; provided that the indemnifying party may not settle any claim that results in the indemnified party's liability and the indemnifying party will be required to consult with the indemnified party during any settlement discussions.

10. LIMITATION OF LIABILITY.

10.1 LIMITATION OF REMEDY. EXCEPT AS PROHIBITED BY LAW, IN NO EVENT WILL EITHER PARTY, ITS AFFILIATES, OR ITS CONTRACTORS, LICENSORS OR SUPPLIERS OR ANY OF THEIR OFFICERS, DIRECTORS, EMPLOYEES, SHAREHOLDERS, AGENTS OR REPRESENTATIVES BE LIABLE TO THE OTHER PARTY, OR ANY OTHER PERSON OR ENTITY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, INDIRECT, EXEMPLARY, OR PUNITIVE DAMAGES OR LIABILITIES

FOR ANY CAUSE WHATSOEVER ARISING OUT OF OR RELATING TO THIS AGREEMENT, INCLUDING ALL STATEMENTS OF WORK, ORDER FORMS, OR AMENDMENTS THERETO, WHETHER IN CONTRACT OR TORT OR BY WAY OF INDEMNITY OR OTHERWISE, INCLUDING A BREACH THEREOF OR INCLUDING DAMAGES OR LIABILITIES FOR LOST PROFIT, LOST REVENUE, LOSS OF USE, LOSS OF GOODWILL, LOSS OF REPUTATION, LOSS OF DATA, REGULATORY FINES, COSTS OF RECREATING LOST DATA, THE COST OF ANY SUBSTITUTE EQUIPMENT, SOFTWARE PROGRAM, OR DATA, REGARDLESS OF WHETHER THE POSSIBILITY OF SUCH DAMAGES OR LIABILITIES HAVE BEEN COMMUNICATED TO SUCH PARTY AND REGARDLESS OF WHETHER SUCH PARTY HAS OR GAINS KNOWLEDGE OF THE EXISTENCE OF SUCH DAMAGES OR LIABILITIES.

10.2 MAXIMUM LIABILITY. EXCEPT (I) FOR THE RECOVERY OF SUMS DUE UNDER THIS AGREEMENT, (II) AS PROHIBITED BY LAW OR (III) FOR CLAIMS ARISING UNDER SECTIONS 1.1 – 1.3(A), 4, 9.1 AND 9.2, IN NO EVENT WILL EITHER PARTY'S LIABILITY FOR ANY DAMAGES TO THE OTHER, ANY OF ITS AFFILIATES, OR TO ANY THIRD PARTY REGARDLESS OF THE FORM OF ACTION, WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, PRODUCTS LIABILITY OR OTHERWISE, EVER EXCEED THE ACTUAL FEES RECEIVED BY SPIRION UNDER THIS AGREEMENT FOR THE PORTION OF THE SPIRION SERVICES GIVING RISE TO SUCH CLAIM DURING THE PRECEDING TWELVE (12) MONTH PERIOD.

11. TERM AND TERMINATION.

11.1 Term and Renewals. The initial term of this Agreement will be as set forth in the Order Form (the "**Initial Term**"), unless earlier terminated in accordance with this Section 11. The Initial Term will automatically renew for successive one year periods commencing on the anniversary of the Effective Date of the Initial Term (each a "**Renewal Term**"; the Initial Term and all Renewal Terms are collectively referred to as the "**Term**"), unless either party notifies the other on or before ninety (90) days prior to the end of the then-current Term.

11.2 Termination for Breach. In the event that either party materially defaults in the performance of any of its duties or obligations under this Agreement and does not substantially cure such default, or commence a cure, within thirty (30) days after being

given written notice specifying the default, the non-defaulting party may, by giving written notice thereof to the defaulting party, terminate this Agreement. Spirion may, by written notice to Customer, terminate Customer's right to use the Services without liability to Customer, if Customer fails to pay the applicable Fees for the Services as set forth in the Order Form Schedule B within thirty (30) days after Spirion gives Customer notice of such nonpayment. Any such suspension or termination of access to the Services does not relieve Customer from paying any past due amounts and any amounts due Spirion through the expiration date of this Agreement.

11.3 Effect of Termination. Within thirty (30) days (or earlier upon Spirion's reasonable written request) after the effective date of a termination of this Agreement for any reason, Customer will (i) pay Spirion for all Services performed by Spirion up to the effective date of such termination and all other amounts owed by Customer to Spirion under this Agreement including, but not limited to, all Fees owed by Customer as of the effective date of termination according to the payment schedule set forth in the Order Form, regardless of the date of termination; and (ii) destroy or return to Spirion all Spirion property, including, but not limited to all Spirion Content, Documentation and Confidential Information. Upon the destruction or return of such materials, Customer will provide Spirion with a signed written statement certifying that it has destroyed or returned all Spirion property to Spirion. Upon termination of this Agreement for any reason, all rights and licenses granted by Spirion hereunder to Customer will immediately cease.

11.4 Return of Customer Data. For up to thirty (30) days after the Term of this Agreement, when requested in writing by Customer, Spirion will deliver, or make available, electronic files containing all available Customer Data. Thirty (30) days following termination of this Agreement, all Customer Data in the System will no longer be available and will be purged from the System.

11.5 Survival. Termination of this Agreement will not affect survival of the provisions regarding either party's treatment of Confidential Information, provisions relating to the payments of amounts due

that have accrued prior to termination, indemnity provisions, provisions limiting or disclaiming the party's liability, or the provisions on termination, which provisions will survive such termination.

12. DISPUTES.

If at any time a dispute arises out of or in connection with this Agreement or any part thereof (e.g., a SOW), then Spirion and Customer will have their respective Project Managers meet in good faith with a view to resolving the dispute within a period of fifteen (15) Business Days from the day the dispute first arises. Should the parties not be able to resolve the dispute within the fifteen (15) Business Days, then both parties will refer the matter to their own appropriate level of senior executive management respectively for resolution. If the relevant senior executive management of Spirion and Customer are unable to resolve the dispute within a further ten (10) Business Day period, then the parties will attempt to settle the dispute through discussions between each parties' respective Chief Executive Officer. In the absence of an amicable resolution within fifteen (15) Business Days from the meeting of the respective Chief Executive Officers in accordance with the conditions set forth in this Section 12, the dispute may then be submitted to the appropriate courts having jurisdiction over the matter as governed by Section 13.6. Nothing in this Agreement will prevent either party from taking such action as it deems appropriate (including any application to a relevant court) for injunctive or other emergency or interim relief in relation to its Intellectual Property Rights or Confidential Information.

13. GENERAL.

13.1 Marketing. Customer agrees to permit Spirion's reasonable reference to Customer's status as a user of the Services, including captioned quotations in product literature or advertisements, websites, articles, press releases, marketing literature, presentations and the like and occasional use as a reference for potential new users.

13.2 Force Majeure. Neither Spirion nor Customer will be liable to the other for any delay or failure to perform (other than a failure to pay monies due under this Agreement) arising out of causes beyond its reasonable control including, but not limited to, riots,

epidemics, severe weather, acts of the other party, fire, flood, terrorism, war, acts of the enemy, embargoes or work stoppages, labor disputes or strikes. Spirion and Customer will notify each other promptly upon learning of any event that may result in any delay or failure to perform. If the force majeure event occurs and continues to prevent substantial performance for more than thirty (30) days, the other party has the right to terminate this Agreement.

13.3 Entire Agreement. This Agreement constitutes the sole and entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the body of this Agreement, the related exhibits, schedules, attachments, and appendices (other than an exception expressly set forth as such therein) and any other documents incorporated herein by reference, the following order of precedence governs: (1) Terms and Conditions, excluding its schedules; (2) the Order; (3) the Schedules, (4) any PSA, and (5) any SOW.

13.4 Assignment. Except as otherwise set forth in this Agreement, this Agreement and all rights and obligations may not be assigned (by operation of law or otherwise) in whole or in part by Customer, and any such attempted assignment will be void and of no effect; provided, however, that either party hereto will have the right to assign this Agreement to another entity in connection with a reorganization, merger, consolidation, acquisition or other restructuring involving all or substantially all of the voting securities and/or assets of the assigning party upon written notice to the non-assigning party. This Agreement will be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors, and assigns as permitted by this Agreement. There are no third-party beneficiaries of this Agreement and, in particular but without limiting the generality of the foregoing, no target or actual customers, or potential or actual employees of Customer or any Customer affiliate will have any legal rights or entitlements of any kind hereunder under any circumstances.

13.5 Waiver and Invalidity. No delay or failure in exercising any right hereunder and no partial or single exercise thereof will be deemed to constitute a waiver of such right or any other rights hereunder. If any provision hereof is declared invalid by a court of competent jurisdiction, such provision will be ineffective only to the extent of such invalidity, so that the remainder of that provision and all remaining provisions of this Agreement will be valid and enforceable to the fullest extent permitted by applicable law.

13.6 Choice of Law. This Agreement will be exclusively construed, governed and enforced in all respects in accordance with the internal laws (excluding all conflict of law rules) of the State of Florida and any applicable federal laws of the United States of America, as from time to time amended and in effect. Each party agrees that any claim or cause of action whether in law or equity, arising under or relating to this Agreement may be brought in a court of appropriate jurisdiction in the State of Florida. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply in any respect to this Agreement or the parties hereto. The parties hereby agree that their respective rights and obligations hereunder will be solely and exclusively as set forth herein and that UCITA, whether enacted in whole or in part by any state or applicable jurisdiction, regardless of how codified, will not apply to this Agreement and is hereby disclaimed.

13.7 Counterparts. This Agreement and any SOW may be executed in any number of counterparts, each of which will be deemed an original but all of which together will be deemed for all purposes to constitute one and the same instrument. Signatures transmitted and received via email will be treated as original signatures for all purposes of this Agreement.

13.8 Government Entities. The Software and Documentation may be deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.72 et. seq. and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government

shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

13.9 Sanctions; Export Controls. Spirion's obligations under this Agreement are subject to the condition that the fulfillment of such obligations are not prohibited by applicable Economic Sanctions Laws or US export control laws. Customer represents and warrants that neither Customer, any Customer Affiliate or any Customer Personnel is (A) included on a Sanctions List or otherwise a target of any Economic Sanctions Laws, (B) directly or indirectly owned or controlled by any Person included on a Sanctions List or otherwise a target of any Economic Sanctions Laws, (C) located, organized or resident in a country or territory that is, or whose government is, the target of any Economic Sanctions Laws, (D) on the Denied Persons List, the Entity List or any similar list maintained by the US Department of Commerce that implements restrictions or prohibitions arising out of US foreign trade and customs requirements, embargoes or sanctions, or (E) to Customer's knowledge, the subject of any investigation by a US governmental entity for violation of Economic Sanctions Laws or US export control laws. If the preceding sentence becomes untrue in whole or in part for any reason during the Term, Customer agrees to notify Spirion promptly and will provide detailed related information to Spirion.

Customer agrees not to act in any manner that would reasonably be expected to result in a violation by Spirion of any Economic Sanctions Law (including using its relationship with Spirion or the Software to facilitate any activities of or business with any Person that is, at the time of such facilitation, on any Sanctions List).

The Software may be, or may become, subject to US export control laws, including the US Export Control Reform Act and its associated regulations. Customer will not directly or indirectly (whether separately or as part of a system), export, re-export, or release the Software or any technical information relating to the Software to, or make the Software or such technical information accessible from, any country,

jurisdiction or Person to which export, re-export, or release is prohibited by applicable laws (including US export control laws) or which would require Spirion to be in violation of such laws in the absence of a license. Customer will at its sole expense comply with all applicable Laws and complete all required undertakings (including obtaining any necessary export license or other governmental approval) prior to exporting, re-exporting, releasing, or otherwise making the Software or technical information relating to the Software available outside the US, and will provide a copy of such licenses or approvals to Spirion upon request.

Customer will fully cooperate with Spirion to confirm or achieve compliance with any Economic Sanctions Laws or US export control laws, and will provide to Spirion promptly upon request any documents that are reasonably related to such compliance (including end-user certificates and affidavits).

13.10 Notices. Any and all notices permitted or required to be given hereunder will be deemed duly effectively given: (a) when received, if delivered by hand, with signed confirmation of receipt; (b) when received, if sent by a nationally recognized overnight courier, signature required; (c) when sent, if by email, (with confirmation of transmission), if sent during the addressee's normal business hours, and on the next Business Day, if sent after the addressee's normal business hours; and (d) on the third day after the date mailed by certified or registered mail, return receipt requested, postage prepaid. Each such notice must be sent to the respective party at the addresses indicated on the signature page. Notice to Spirion must include a copy to: legal@spirion.com.

Schedule A

Definitions

- 2.1 **“Access Credentials”** means the username, password, active directory authentication, or other security code, method, technology, or device used, alone or in combination, to verify an individual’s identity and authorization to access and use the Services.
- 2.2 **“Authorized Users”** means Customer’s employees, consultants, contractors, and agents (a) who are authorized by Customer to access and use the Services under the rights granted to Customer pursuant to this Agreement; and (b) for whom access to the Services has been purchased hereunder.
- 2.3 **“Business Day”** collectively means Monday through Friday of each week, other than days on which banks in New York, New York, U.S.A, are closed for banking and any other date designated by Spirion as a company holiday (taking into account that different holidays may be recognized on different days each year);
- 2.4 **“Confidential Information”** means any information or material in tangible or intangible form that: (i) is confidential and proprietary to the disclosing party, possesses an element of value to the disclosing party, is not generally known to the disclosing party’s competitors, and would damage the disclosing party if disclosed; or (ii) the disclosing party obtains from any third party and which the disclosing party treats as proprietary whether or not such information or material is owned by the disclosing party;
- 2.5 **“Customer Affiliate”** means any entity controlling, controlled by, or under common control with Customer, where the root word “control” means (i) owning forty percent or more of an entity’s voting securities, partnership interests, membership interests or the like, (ii) having the right to appoint forty percent or more of an entity’s Board of Directors or similar governing body or (iii) having the right to forty percent or more of the profits of an entity or forty percent or more of the assets of an entity upon dissolution.
- 2.6 **“Customer Data”** means information, data, and other content, in any form or medium, that is received, directly or indirectly from Customer or an Authorized User by or through the Services, or that incorporates or is derived from the Processing of such data by the Services, namely, the data delivered in Reports. For the avoidance of doubt, Customer Data does not include Resultant Data or any other information reflecting the access or use of the Services by or on behalf of Customer or any Authorized User.
- 2.7 **“Customer Personnel”** means, with regard to any Customer Affiliate, the officers, directors, agents, representatives, contractors and employees of that entity, collectively and individually.
- 2.8 **“Customer Systems”** means the Customer’s information technology infrastructure, including computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Customer or through the use of third-party services.
- 2.9 **“Deliverables”** means those Services detailed in a Statement of Work.
- 2.10 **“Derivative Works”** means any suggestions, contributions, enhancements, improvements, modifications or changes to the referenced materials.
- 2.11 **“Documentation”** means the user documentation and any other operating, training, and reference manuals relating to the use of the Services, as supplied by Spirion to Customer, as well as any Derivative Works thereto;
- 2.12 **“Economic Sanctions Law”** means any statute, law, ordinance, regulation, rule, code, governmental order, executive order, guidance or other requirement or rule of law that imposes economic sanctions and trade embargoes and is administered by OFAC or any successor US governmental entity and, if Licensee is a business organized outside of the United States, such laws in the country of organization of Licensee.
- 2.13 **“Intellectual Property Rights”** means all rights in and to any of the following, however constituted: trade secrets, patents, copyrights, trademarks, service marks, URLs, trade dress, brand features, know-how, moral rights, contract rights, code (executable, source and other) and similar rights of any type under the laws of any applicable governmental authority, or international treaty, including, without limitation, all applications and registrations relating to any of the foregoing;

- 2.14 **“Order Form”** means the initial order form set forth in Schedule A as well as subsequent order forms, which will serve as the mechanism by which Customer may purchase additional Services following the Effective Date that incorporates the terms and conditions of this Agreement;
- 2.15 **“Permitted Use”** means any use of the Services by an Authorized User for the purpose of discovering, classifying, and monitoring, certain Sensitive Data located on servers and devices within Customer Systems.
- 2.16 **“Person”** means any individual, corporation, limited liability company, partnership, association or other entity.
- 2.17 **“Personal Data”** means (i) that subset of Customer Data that relates to or can be attributed to an identified or identifiable natural person and/or (ii) information concerning an identified or identifiable natural person that is protected by applicable laws.
- 2.18 **“Process”** means to take any action or perform any operation or set of operations that the SaaS Services are capable of taking or performing on any data, information, or other content, including but not limited to receive, store, organize, evaluate, analyze, sort, anonymize, process, retrieve, transmit, or otherwise use. **“Processing”** and **“Processed”** have correlative meanings.
- 2.19 **“Professional Services”** means the services provided by Spirion for Customer pursuant to a Statement of Work (Schedule E).
- 2.20 **“Reporting”** means the part of the reports regarding the processing of the Customer Data by the Services (“Reports”).
- 2.21 **“Resultant Data”** means data and information related to Customer’s use of the Services that is used by Spirion in an aggregate and anonymized manner, including to compile statistical and performance information related to the provision and operation of the Services.
- 2.22 **“Sanctions List”** means the “Specially Designated Nationals and Blocked Persons List”, the “Consolidated Sanctions List” and any other list that is not included in the forgoing lists that identifies targets of Economic Sanctions Laws and is maintained by OFAC or any successor US governmental entity.
- 2.23 **“Sensitive Data”** means the categories of data, including but not limited to Personal Data, to be identified by the Services, as selected by Customer, such as Social Security number or credit card number.
- 2.24 **“Services”** means the software-as-a-service offering(s) listed on the Order Form. Each offering discovers Sensitive Data within the Customer Data provided by Customer to Spirion, and delivers Reports requested by the Customer;
- 2.25 **“Specifications”** means the specifications set forth in the Documentation;
- 2.26 **“Spirion Materials”** means the Services, Specifications, Documentation, and Spirion Systems and any and all other information, data, documents, materials, works, and other content, devices, methods, processes, hardware, software, and other technology in the hosting servers and inventions, including the Spirion user interface, any deliverables, technical or functional descriptions, requirements, plans, or reports (including the look and feel of Reports), that are provided by or used by Spirion in connection with the Services or otherwise comprise or relate to the Services or Spirion Systems. For the avoidance of doubt, Spirion Materials include Resultant Data and any information, data, or other content derived from Spirion’s monitoring of Customer’s access to or use of the Services, but do not include Customer Data.
- 2.27 **“Spirion Server”** means any server used by Spirion to provide the Services, including Microsoft Azure cloud servers that Spirion currently uses to provide the Service;
- 2.28 **“Spirion Services”** means the collective reference to all services Spirion performs for Customer under this Agreement and includes without limitation, any Professional Services provided under an SOW;
- 2.29 **“Spirion Systems”** means the information technology infrastructure used by or on behalf of Spirion in performing the Services, including all computers, software, hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Spirion or through the use of third-party services.
- 2.30 **“Term”** has the meaning set forth in Section 13.1 of this Agreement.
- 2.31 **“Third-Party Materials”** means materials and information, in any form or medium, including any open source or other software, documents, data, content, specifications, products, equipment, or

components of the Services that are not proprietary to Spirion.

Schedule B
Order Form

Schedule C

Customer Support Services and SLAs

Schedule D

Data Privacy and Security Addendum

Schedule E
Professional Services SOW

SPIRION SOFTWARE LICENSE AGREEMENT

This SOFTWARE LICENSE AGREEMENT (the "Agreement") is made and entered into effective as of _____ [DATE] ("Effective Date"), by and between SPIRION, LLC, a Delaware Limited Liability Company with its principal place of business at 200 Central Ave., Suite 1900, St. Petersburg, FL 33701 ("Spirion"), and _____ [NAME], its affiliates, employees, contractors or agents ("Licensee"), a _____ [CORPORATE TYPE] with offices at _____ [ADDRESS] (each a "Party" and sometimes jointly referred to herein as the "Parties") and sets forth the terms and conditions under which Spirion will license the Licensed Products to Licensee.

WHEREAS, Spirion desires to license the Software identified on a License Quote to Licensee; and

WHEREAS, Licensee desires to obtain a license to use the Software for its internal business purposes, subject to the terms and conditions of this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. **The Software and Data.** The Parties agree and understand that the Spirion Software is a tool to discover, segregate, and encrypt certain data on Licensee Devices per Licensee's instructions. The Software is to be installed and maintained on-premises on Licensee's computer systems. The Licensee decides which types of Licensee Data it wishes to discover on its devices, for example, credit card numbers. The Software does not transmit Licensee Data to Spirion.

2. **Definitions.**

"**Authorized Technical Contacts**" means the two representatives of the Licensee who are authorized to receive communication from Spirion regarding the Licensed Products or this Agreement.

"**Device**" means an electronic device owned or leased by Licensee or an Employee which is capable of executing the Software program.

"**Defect**" means the failure of the Software to substantially conform to the Documentation, when such failure can be reproduced and documented by Spirion.

"**Documentation**" means product user guides (at URL: www.spirion.com/support/user-guides) relating to the Software that Spirion provides or makes available to Licensee which describe the functionality, components, features, or requirements of the Software, including any aspect of the installation, configuration, integration, operation, or use of the Software.

"**Employee**" or means an employee or authorized contractor of the Licensee whose job functions require the individual to access or store data on one or more Devices.

"**Intellectual Property Rights**" means all rights in and to any of the following, however constituted: trade secrets, patents, copyrights, service marks, trademarks, domain names, trade dress, know-how, moral rights, code (executable, object and other) and related and similar rights under the laws of any applicable governmental authority or international treaty, including but not limited to all applications and registrations relating to the foregoing.

License Types:

"**Lifetime License**" means a license to use the current version of the Software and Documentation in perpetuity. The Lifetime License does not include Maintenance or Support, but Licensee may purchase Maintenance and Support on an annual basis.

"**Annual License**" means a license to use the Software and Documentation for a Term of one year. It includes any Maintenance Releases released during the Term and Support.

"**Licensee Data**" means any data stored on Devices, not including Usage Data.

“**License Quote**” means the Spirion document presented to Licensee that lists the Term, fees, licensed Software, and any Maintenance and Support.

“**Licensed Product(s)**” means the licensed Software and related Documentation.

“**Maintenance Release**” means any update, upgrade, release, or other adaptation or modification of the Software, including any updated Documentation, that Spirion may make available to Licensee from time to time during the Term, which may contain, among other things, bug fixes, error corrections, enhancements, improvements, or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency, or quality of the Software, but does not include any New Version.

“**New Version**” means any new version of the Software that Spirion may from time to time introduce and market generally as a distinct licensed product (as may be indicated by Spirion’s designation of a new version number), and which Spirion may make available to Licensee at an additional cost under a separate written agreement.

“**Permitted Use**” means the use of the Licensed Products by Licensee on its own computer systems for the purpose of discovering sensitive data contained in Licensee Data.

“**Software**” means the executable, object code version of the computer software program(s) identified on a License Quote, and all Maintenance Releases to it made available by Spirion to Licensee during the Term.

“**Support**” is defined in Section 7.

“**Supported Platforms**” means the operating systems that Spirion provides Support for.

“**Term**” means the time period of the License as stated on the License Quote or other Addendum.

“**Usage Data**” means records of how Licensee is using the Software.

“**Website**” means the website at www.spirion.com and any successor URL.

3. License Quotes. Each License Quote or purchase order executed by the Parties shall be incorporated into this Agreement and considered an addendum hereto (“Addenda”). In the event of any conflict between the terms of this Agreement and the terms of an Addendum, the terms of the Agreement shall govern, unless the Addendum expressly identifies the provision of this Agreement it supersedes.

4. License.

4.1 **License Grant.** Subject to and conditioned on Licensee’s payment of fees and compliance with all other terms and conditions of this Agreement, Spirion hereby grants to Licensee a non-exclusive, non-transferable, non-sublicensable, worldwide license to use the Licensed Products solely for the Permitted Use during the Term.

4.2 **Scope of License.** Licensee may install, use, and run one copy of the Software across all of the Devices owned or leased by the number of Employees stated in the License Quote. This copy will remain the exclusive property of Spirion, and its use shall be subject to this Agreement. Licensee must include all copyright and other Intellectual Property notices contained in the original. No other copying is permitted.

4.3 **Third Party Licenses.** The Licensed Products may include software products licensed from third parties. Such third parties have no obligations or liability to Licensee under this Agreement. Specific third-party license terms applying to portions of the Licensed Products are set forth at the following URL: www.spirion.com/Company/ThirdPartyLicensing and are hereby incorporated by reference.

4.4 **Security Measures.** The Software may contain technological measures designed to prevent unauthorized or illegal use of the Software. Licensee acknowledges and agrees that: (a) Spirion may use these and other lawful measures to verify Licensee’s compliance with the terms of this Agreement and enforce Spirion’s rights, including all Intellectual Property Rights, in and to the Software; and (b) Spirion may collect, maintain, process and use diagnostic, technical, usage and related information, including information about Licensee’s computers, systems and software, that Spirion may gather periodically to improve the performance of the Software or develop Maintenance Releases.

4.5 **License Restrictions.** Except as this Agreement expressly permits, Licensee shall not, and shall not permit any other person or entity to:

- (a) copy the Software, in whole or in part;
- (b) modify, correct, adapt, translate, enhance, or otherwise prepare derivative works or improvements of any Software;
- (c) rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer, or otherwise make available the Software to any third party;
- (d) reverse engineer, disassemble, decompile, decode, or adapt the Software, or otherwise attempt to derive or gain access to the source code of the Software, in whole or in part;
- (e) bypass or breach any security device or protection used for or contained in the Software or Documentation;
- (f) remove, delete, efface, alter, obscure, translate, combine, supplement, or otherwise change any trademarks, terms of the Documentation, warranties, disclaimers, or Intellectual Property Rights, proprietary rights or other symbols, notices, marks, or serial numbers on or relating to any copy of the Software or Documentation;
- (g) use the Software in any manner or for any purpose that infringes, misappropriates, or otherwise violates any Intellectual Property Right or other right of any person or entity, or that violates any applicable Law;
- (h) use the Software for purposes of: (i) benchmarking or competitive analysis of the Software; (ii) developing, using, or providing a competing software product or service; or (iii) any other purpose that is to Spirion's detriment or commercial disadvantage; or
- (i) use the Software in or in connection with the design, construction, maintenance, operation, or use of any hazardous environments, systems, or applications, any safety response systems or other safety-critical applications, or any other use or application in which the use or failure of the Software could lead to personal injury or severe physical or property damage.

4.6 Licensee may use the Software to search the data only on the Devices of the number of Employees authorized by this Agreement. If an Employee leaves the employment of or engagement with the Licensee, Licensee may reallocate the use of the Software to include another Employee.

5. **Delivery.** Spirion shall deliver license keys or activation codes to Licensee within ten (10) days of the Effective Date. Licensee shall be responsible for the security of all access credentials.

6. **Maintenance.** During the Term, to the extent Licensee has purchased Maintenance, Spirion will provide Licensee with all Maintenance Releases (including updated Documentation) that Spirion may, in its sole discretion, make generally available to its licensees at no additional charge. All Maintenance Releases provided by Spirion to Licensee are deemed Software. Licensee will install all Maintenance Releases as soon as practicable after receipt. Licensee does not have any right hereunder to receive any New Versions of the Software that Spirion may, in its sole discretion, release from time to time. Licensee may license any New Version at Spirion's then-current list price and subject to a separate license agreement, provided that Licensee is in compliance with the terms and conditions of this Agreement.

7. **Support.** During the Term, to the extent Licensee has purchased Support, Spirion shall offer Support on the then current general release of the Software, as well as the most recent Maintenance Releases to the prior general release. "**Support**" means:

- (a) Email or Website service ticket support service from 9:00 AM - 5:00 PM (Eastern Time), Monday through Friday except public holidays. Directions for submitting support requests can be found at <http://support.spirion.com>. Tickets may be opened only by Authorized Technical Contacts.
- (b) Spirion's efforts to correct Defects in the then-current release of the Software.
- (c) Support shall not include on-site services.

With sixty (60) days' advance written notice, Spirion may change its Support policy from time to time provided that Support features and services are not reduced.

8. **Payment.** Licensee agrees to pay Spirion all applicable Fees set forth in the License Quote, on the schedule (if any) stated in the License Quote. Payment is due in U.S. dollars, thirty (30) days after invoice date.

8.1 Fees do not include any taxes. Licensee is responsible for all taxes imposed by any governmental authority, other than any taxes on Spirion's income.

8.2 Licensee shall pay Spirion a late charge of the lesser of 3% per month or the highest amount permitted by applicable law on all payments past due. Licensee shall reimburse Spirion for all costs incurred by Spirion in collecting any late payment of amounts due or related interest, including attorneys' fees, court costs, and collection agency fees. If such failure continues for thirty (30) days following written notice thereof, Spirion may: (i) disable Licensee's use of the Software (including by means of a disabling code, technology or device); (ii) withhold, suspend or revoke its grant of a license hereunder; and/or (iii) terminate this Agreement under Section 10.1.

9. **License Compliance Measures; Audit Rights and Remedies.**

9.1 The Software may contain technological copy protection or other security features designed to prevent unauthorized use of the Software. Licensee shall not, and shall not attempt to, remove, disable, circumvent or otherwise create or implement any workaround to, any such copy protection. No more than once annually and with no fewer than ten (10) business days' advance written notice, Spirion may audit Licensee's use of the Software to ensure Licensee's compliance with this Agreement. Spirion shall conduct audits only during Licensee's normal business hours and in a manner that does not unreasonably interfere with Licensee's business operations. If the audit determines that Licensee's use of the Software exceeded the usage permitted by this Agreement by more than 5%, Licensee shall pay to Spirion all amounts due for such excess use of the Software, plus interest on such amounts, as calculated pursuant to the applicable License Quote. If the audit determines that such excess use equals or exceeds 10% percent of Licensee's permitted level of use, Licensee shall also pay to Spirion all reasonable costs incurred by Spirion in conducting the audit. Licensee shall make all payments required under this Section 9.1 within thirty (30) days of the date of written notification of the audit results.

9.2 Spirion reserves the right to remotely disable the Software if it reasonably and in good faith suspects gross abuse or fraud by Licensee, and has attempted to notify Licensee, and the Licensee has not cured the abuse or fraud within thirty (30) days.

10. **Term, Renewal, and Termination.**

10.1 Term. This Agreement shall begin on the Effective Date shall remain in effect for the term stated in each Addenda until it expires or is terminated in accordance with this Agreement ("**Term**"). Either Party shall have the right to terminate this Agreement as to all Addenda or only the applicable Addendum in the event the other Party commits a material breach of any provision of this Agreement ("**Breach**") which remains uncured after thirty (30) days' written notice, or in accordance with any other provisions of this Agreement expressly giving rise to a right of termination. Spirion may terminate this Agreement, effective immediately, if the Licensee (i) is dissolved or liquidated or takes any corporate action for such purpose; (ii) becomes insolvent or is generally unable to pay its debts as they become due; (iii) becomes the subject of any voluntary or involuntary bankruptcy proceeding under any domestic or foreign bankruptcy or insolvency law; (iv) makes or seeks to make a general assignment for the benefit of its creditors; or (v) applies for, or consents to, the appointment of a trustee, receiver or custodian for a substantial part of its property.

10.2 Renewal. Annual Licenses, Maintenance, and Support, will automatically renew unless earlier terminated pursuant to any of the Agreement's express provisions or either Party gives the other Party written notice of non-renewal at least sixty (60) days prior to the expiration of the then-current term (each a "**Renewal Term**" and, collectively, together with the initial Term, the "**Term**").

10.3 Effect of Termination and Expiration. Upon termination of this Agreement resulting from an uncured Breach by Spirion, Spirion agrees to refund to Licensee any unused Fees (as applicable), pro-rated on a 12-month term. Upon expiration or termination of this Agreement for any reason, Licensee shall remove and destroy all copies of the Software installed on all Devices, and remove and destroy all copies of the Documentation in its possession. Licensee shall direct all Employees with a copy of the Software installed

on a personally owned Device, if any, to remove and destroy such Software and remove and destroy all copies of the Documentation in such Employees' possession.

10.4 **Survival.** The provisions set forth in the following sections, and any other right, obligation or provision under this Agreement that, by its nature, should survive termination or expiration of this Agreement, will survive any expiration or termination of this Agreement: Sections 10, 12, 14, 15, and 16.

11. **Public Announcements.** Spirion may identify Licensee by name and/or logo to the public as a customer of Spirion. Spirion may also issue one or more press releases announcing Licensee's execution of this Agreement and the implementation of the Software. Spirion may also publicly issue a case study describing Licensee's use of the Software.

12. **Intellectual Property Rights.** Licensee acknowledges and agrees that the Licensed Products and all related Intellectual Property Rights are the exclusive property of Spirion and its licensors. The Software and Documentation are licensed, not sold, to Licensee by Spirion and Licensee does not have under or in connection with this Agreement any ownership interest in the Software or Documentation, or in any related Intellectual Property Rights. Spirion and its licensors are the sole and exclusive owners of all right, title, and interest in and to the Software and Documentation, including all Intellectual Property Rights relating thereto, and any derivative works or improvements created by. Licensee hereby unconditionally and irrevocably assigns to Spirion or Spirion's designee, its entire right, title, and interest in and to any Intellectual Property Rights that Licensee may now or hereafter have in or relating to the Software or Documentation (including any rights in derivative works or patent improvements relating to either of them, authorized or not).

13. **Warranties and Disclaimers.**

13.1 **Warranties.** Each Party warrants that it has full legal right to enter into this Agreement. Spirion warrants that the Software, if installed and operated in accordance with the Documentation, will perform substantially in conformance with the Documentation, for a period of six (6) months provided that Licensee has installed all Maintenance Releases previously made available to Licensee, and further provided that Licensee is in compliance with all terms and conditions of this Agreement.

13.2 **Disclaimers.** Licensee agrees that the Software uses search algorithms to find data but is not guaranteed to find all instances of data searched for. LICENSEE ACKNOWLEDGES THAT USING THE SOFTWARE, EVEN AS DIRECTED, DOES NOT GUARANTEE COMPLIANCE WITH ANY PARTICULAR LAW, REGULATION, STANDARD, OR BEST PRACTICE, EACH OF WHICH SPIRION EXPRESSLY DISCLAIMS TO THE FULLEST EXTENT OF THE LAW. SPIRION SHALL NOT BE LIABLE UNDER ANY THEORY FOR LICENSEE'S VIOLATION OR BREACH OF ANY LAW, REGULATION OR STANDARD, EVEN IF SUCH VIOLATION OR BREACH INVOLVED LICENSEE'S USE OF THE SOFTWARE. EXCEPT FOR THE LIMITED WARRANTIES SET FORTH IN SECTION 13.1, ALL LICENSED SOFTWARE AND DOCUMENTATION AND OTHER PRODUCTS, INFORMATION, MATERIALS, AND SERVICES PROVIDED BY SPIRION ARE PROVIDED "AS IS." SPIRION DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

EXCEPT AS SET FORTH ELSEWHERE IN THIS AGREEMENT, LICENSEE ASSUMES RESPONSIBILITY FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, SPIRION MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR ACHIEVE ANY INTENDED RESULT. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO LICENSEE.

14. **Infringement Claims; Indemnification.**

14.1 **Indemnification by Spirion.** Spirion shall indemnify, defend and hold Licensee harmless from and against any claims, losses, damages, liabilities, costs and expenses (including reasonable attorneys' fees and costs) arising out of any claim, suit or proceeding brought by a third party against Licensee, which alleges that the Licensed Products, as delivered and used in accordance with the terms and conditions of this Agreement and the Documentation, infringe any third party Intellectual Property Rights. Licensee agrees to notify Spirion of any such claim promptly in writing, tender the defense to Spirion and to allow Spirion to manage, control, and/or settle the proceedings, provided that Spirion will not settle such claim or related action in a manner that imposes any obligation on Licensee without the prior written consent of Licensee (which consent will not be unreasonably withheld). Licensee agrees to

cooperate fully with Spirion during such proceedings. Spirion shall have no obligation or liability to Licensee with respect to any claim of infringement which is based upon: (i) the combination or modification of the Software by Licensee with any other product, application, process, program or device not provided by Spirion (excluding combinations described in the Documentation), if such infringement would not have arisen but for such combination or modification, or (ii) the failure of Licensee to promptly install a Maintenance Release provided by Spirion where such infringement could have been avoided by the use of such Maintenance Release, or (iii) use of Software by Licensee in a manner other than for which it was designed or in a manner other than as specified in the Documentation.

14.2 **Indemnification by Licensee.** Licensee shall indemnify, hold harmless and defend Spirion, its affiliates, and their respective officers, directors, employees, managers, advisors, agents, and attorneys, harmless from and against any claims, losses, damages, liabilities, costs and expenses (including reasonable attorneys' fees and costs) arising out of any claim, suit or proceeding brought by a third party regarding (a) the use of the Licensed Products in a manner not expressly permitted under this Agreement; or (b) Licensee's breach of this Agreement. Spirion agrees to notify Licensee of any such claim promptly in writing, tender the defense to Licensee and to allow Licensee to manage, control, and/or settle the proceeding, provided that Licensee will not settle such claim or related action in a manner that imposes any obligation on Spirion without the prior written consent of Spirion (which consent will not be unreasonably withheld). Spirion agrees to cooperate fully with Licensee during such proceedings.

14.3 **Mitigation.** In the event of an infringement claim or should Spirion have reasonable concerns about infringement or potential infringement, Spirion may, at Spirion's option, replace, in whole or in part, the Licensed Products of concern (the "Affected Licensed Products") with a substantially compatible and functionally equivalent computer program or programs, modify the Affected Licensed Products to avoid the infringement and/or obtain such license(s) as it deems appropriate. Licensee agrees to promptly install any such replacement version(s) and discontinue use of the superseded version(s). Licensee further agrees to promptly direct all Employees with Software installed on a personally owned Device to promptly install any such replacement version(s) and discontinue the use of the superseded version(s) on such personally owned Devices. If Spirion reasonably determines that other alternatives are not available at a cost that Spirion deems acceptable, Spirion may, at its option, terminate the license to the Licensed Product on thirty (30) days' notice, in which case, Spirion refund any Licensee, Maintenance, or Support Fees pro-rated on a 12-month term.

14.4 **Sole Remedy.** THIS SECTION 14 SETS FORTH LICENSEE'S SOLE REMEDIES AND SPIRION'S SOLE LIABILITY AND OBLIGATION FOR ANY ACTUAL, THREATENED, OR ALLEGED CLAIMS THAT THE SOFTWARE OR DOCUMENTATION OR ANY SUBJECT MATTER OF THIS AGREEMENT INFRINGES, MISAPPROPRIATES, OR OTHERWISE VIOLATES ANY INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

15. **Limitation of Liability.** EXCEPT FOR THE INDEMNITY OBLIGATIONS IN SECTION 14, UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL SPIRION OR ITS LICENSORS OR SUPPLIERS BE LIABLE TO LICENSEE OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES.

IN NO EVENT WILL SPIRION BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE FEES ACTUALLY PAID BY LICENSEE, EVEN IF SPIRION SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY.

16. **Miscellaneous.**

16.1 **Notice.** Any notice or other communication to be given pursuant to this Agreement shall be in writing and shall be effective either when delivered personally to the other Party, or one business day following sending by overnight courier service, addressed to such Party at the address set forth below, signature proving receipt required.

Spirion, LLC
200 Central Ave., Suite 1900
St. Petersburg, FL 33701

Licensee: _____
Address: _____
Attn: _____

Email: sales@spirion.com

Email: _____

With a copy to: legal@spirion.com

16.2 **Headings and Rules of Construction.** Section headings are for convenience of reference only and shall not affect the construction or interpretation of this Agreement. Whenever used herein, the singular includes the plural and the plural includes the singular. The use of any gender, tense or conjugation includes all genders, tenses and conjugations.

16.3 **United States Government.** The Licensed Products are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.72 et. seq. and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

16.4 **Export Controls.** The Software may be subject to US export control laws, including the US Export Control Reform Act and its associated regulations. Licensee will not directly or indirectly, export, re-export, or release the Software to, or make the Software accessible from, any country, jurisdiction or Person to which export, re-export, or release is prohibited by applicable Law. Licensee will comply with all applicable Laws and complete all required undertakings (including obtaining any necessary export license or other governmental approval) prior to exporting, re-exporting, releasing, or otherwise making the Software available outside the US.

16.5 **Suggestions and Feedback.** Either Party may from time to time provide suggestions, comments or other feedback to the other Party with respect to Licensed Products or any other subject ("Feedback"). Both Parties agree that all Feedback is and shall be entirely voluntary and shall not, absent separate agreement, create any confidentiality obligation for the receiving Party. Feedback may or may not be clearly designated as such and, except as otherwise provided herein, each Party shall be free to disclose, use, or commercially exploit such Feedback as it sees fit, entirely without obligation of any kind to the other Party. Licensee obtains no Intellectual Property Rights, title, or interest in the Licensed Products, even if such intellectual property incorporates Feedback from Licensee.

16.6 **Governing Law; Submission to Jurisdiction.** This Agreement is governed by and construed in accordance with the internal laws of the State of Florida without giving effect to any choice or conflict of law provision or rule that would require or permit the application of the laws of any jurisdiction other than those of the State of Florida. Any legal suit, action, or proceeding arising out of or related to this Agreement or the licenses granted hereunder will be instituted exclusively in the federal courts of the United States or the courts of the State of Florida located in the city of Tampa and County of Pinellas, respectively, and each Party irrevocably submits to the exclusive jurisdiction and venue of such courts in any such suit, action, or proceeding. Service of process, summons, notice, or other document by mail to such Party's address set forth herein will be effective service of process for any suit, action, or other proceeding brought in any such court. The parties agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement or to the parties to this Agreement. The parties also agree that the Uniform Computer Information Transactions Act (UCITA), whether enacted in whole or in part by any state or applicable jurisdiction, regardless of how codified, will not apply to this Agreement.

16.7 **Waiver of Jury Trial.** THE PARTIES HEREBY WAIVE THEIR RIGHTS TO A TRIAL BY JURY.

16.8 Waiver. No waiver by either Party of any of the provisions of this Agreement will be effective unless explicitly set forth in writing and signed by the waiving Party. Except as otherwise set forth in this Agreement, no failure to exercise, or delay in exercising, any rights, remedy, power or privilege arising from this Agreement shall operate or be construed as a waiver thereof.

16.9 Assignment. Licensee agrees not to assign, or otherwise transfer this Agreement or such Party's rights under it, or delegate its obligations, without Spirion's prior written consent, and any attempt to do so is void. Licensee may assign this Agreement without prior written consent only to an entity which acquires all or substantially all of its assets. Any other attempt to assign is void, without written consent from Spirion.

16.10 Relationship of the Parties. The relationship between the Parties is that of independent contractors. Nothing contained in this Agreement will be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, employment, or fiduciary relationship between the Parties, and neither Party shall have authority to contract for or bind the other Party in any manner whatsoever.

16.11 Force Majeure. Neither Party shall be responsible for any delay or failure of performance under this Agreement caused by events or circumstances beyond such Party's control, which may not be overcome by due diligence.

16.12 Severability. If any provision of this Agreement is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability will not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. On such determination that any term or other provision is invalid, illegal, or unenforceable, the Parties hereto shall negotiate in good faith to modify this Agreement so as to effect the original intent of the Parties.

16.13 Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same agreement. Authorized signatures transmitted and received via electronic means will be treated as original signatures for all purposes of this Agreement.

16.14 Remedies. The rights and remedies of Spirion provided in this Agreement shall be in addition to (and not in substitution for) any rights and remedies to which Spirion shall be entitled at law or equity.

16.15 Amendments or Modifications. This Agreement may not be modified except in an amendment executed by duly authorized representatives of the Parties. The terms and conditions of this Agreement (including Addenda and attached exhibits) shall supersede all conflicting pre-printed terms and conditions contained in any purchase order or other business form submitted by either Party to the other.

16.16 No Third-Party Beneficiaries. This Agreement is for the sole benefit of the Parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or will confer on any other Person any legal or equitable right, benefit, or remedy of any nature whatsoever under or by reason of this Agreement. Licensee and Spirion are the only parties to this Agreement.

16.17 Entire Agreement. This Agreement, including all Addenda and attached exhibits, sets forth the entire agreement between the Parties concerning the subject matter hereof and supersedes all prior agreements, negotiations, discussions, arrangements and communications, whether oral or written, with respect to the subject matter hereof.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

Spirion, LLC **Licensee**

By:	By:
Name:	Name:
Title:	Title:

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**

(c) Uses net proceeds to maintain, improve, or expand the operations of the organization.

Obligations means, when used in connection with a non-Federal entity's utilization of funds under a Federal award, orders placed for property and services, contracts and subawards made, and similar transactions during a given period that require payment by the non-Federal entity during the same or a future period.

Pass-through entity means a non-Federal entity that provides a subaward to a subrecipient to carry out part of a Federal program.

Recipient means a non-Federal entity that receives a Federal award directly from a Federal awarding agency to carry out an activity under a Federal program. The term recipient does not include subrecipients.

Simplified acquisition threshold means the dollar amount below which a non-Federal entity may purchase property or services using small purchase methods. Non-Federal entities adopt small purchase procedures in order to expedite the purchase of items costing less than the simplified acquisition threshold. The simplified acquisition threshold is set by the Federal Acquisition Regulation at 48 CFR Subpart 2.1 (Definitions) and in accordance with 41 U.S.C. 1908. As of the publication of this part, the simplified acquisition threshold is \$150,000, but this threshold is periodically adjusted for inflation. (Also see definition of § 200.67 Micro-purchase.)

Subaward means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

Subrecipient means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency.

Termination means the ending of a Federal award, in whole or in part at any time prior to the planned end of period of performance.

The following certifications and provisions may be required and apply when Participating Agency expends federal funds for any purchase resulting from this procurement process. Pursuant to 2 C.F.R. § 200.326, all contracts, including small purchases, awarded by the Participating Agency and the Participating Agency's subcontractors shall contain the procurement provisions of Appendix II to Part 200, as applicable.

APPENDIX II TO 2 CFR PART 200

(A) Contracts for more than the simplified acquisition threshold currently set at \$150,000, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Pursuant to Federal Rule (A) above, when a Participating Agency expends federal funds, the Participating Agency reserves all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party.

Does offeror agree? YES TH Initials of Authorized Representative of offeror

(B) Termination for cause and for convenience by the grantee or subgrantee including the manner by which it will be effected and the basis for settlement. (All contracts in excess of \$10,000)

Pursuant to Federal Rule (B) above, when a Participating Agency expends federal funds, the Participating Agency reserves the right to immediately terminate any agreement in excess of \$10,000 resulting from this procurement process in the event of a breach or default of the agreement by Offeror as detailed in the terms of the contract.

Does offeror agree? YES TH Initials of Authorized Representative of

OMNIA PARTNERS EXHIBITS

EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

offeror

(C) Equal Employment Opportunity. Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 CFR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

Pursuant to Federal Rule (C) above, when a Participating Agency expends federal funds on any federally assisted construction contract, the equal opportunity clause is incorporated by reference herein.

Does offeror agree to abide by the above? YES TH Initials of Authorized Representative of offeror

(D) Davis-Bacon Act, as amended (40 U.S.C. 3141-3148). When required by Federal program legislation, all prime construction contracts in excess of \$2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay wages not less than once a week. The non-Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency. The contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

Pursuant to Federal Rule (D) above, when a Participating Agency expends federal funds during the term of an award for all contracts and subgrants for construction or repair, offeror will be in compliance with all applicable Davis-Bacon Act provisions.

Does offeror agree? YES TH Initials of Authorized Representative of offeror

(E) Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708). Where applicable, all contracts awarded by the non-Federal entity in excess of \$100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

Pursuant to Federal Rule (E) above, when a Participating Agency expends federal funds, offeror certifies that offeror will be in compliance with all applicable provisions of the Contract Work Hours and Safety Standards Act during the term of an award for all contracts by Participating Agency resulting from this procurement process.

Does offeror agree? YES TH Initials of Authorized Representative of offeror

(F) Rights to Inventions Made Under a Contract or Agreement. If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small

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 _____ TH _____ 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 _____ TH _____ 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 _____ TH _____ 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 TH 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 TH 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 TH 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 TH 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 TH 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 TH 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: Spirion, LLC

Address, City, State, and Zip Code:
200 Central Ave St 1900, St Petersburg, 33701

OMNIA PARTNERS EXHIBITS
EXHIBIT F - FEDERAL FUNDS CERTIFICATIONS

Phone Number: 503 522 5453 Fax Number: _____

Printed Name and Title of Authorized
Representative: Ty Hurner

Email Address: ty.hurner@spirion.com

Signature of Authorized Representative: *Ty Hurner* Date: 11/20/2020

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' 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
DOC #8	Equal Employment Opportunity/Affirmative Action Evidence
DOC #9	McBride Principles

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.

STATEMENT OF OWNERSHIP DISCLOSURE

N.J.S.A. 52:25-24.2 (P.L. 1977, c.33, as amended by P.L. 2016, c.43)

This statement shall be completed, certified to, and included with all bid and proposal submissions. Failure to submit the required information is cause for automatic rejection of the bid or proposal.

Name of Organization: _____

Organization Address: _____

Part I Check the box that represents the type of business organization:

- Sole Proprietorship (skip Parts II and III, execute certification in Part IV)
- Non-Profit Corporation (skip Parts II and III, execute certification in Part IV)
- For-Profit Corporation (any type) Limited Liability Company (LLC)
- Partnership Limited Partnership Limited Liability Partnership (LLP)
- Other (be specific): _____

Part II

The list below contains the names and addresses of all stockholders in the corporation who own 10 percent or more of its stock, of any class, or of all individual partners in the partnership who own a 10 percent or greater interest therein, or of all members in the limited liability company who own a 10 percent or greater interest therein, as the case may be. **(COMPLETE THE LIST BELOW IN THIS SECTION)**

OR

No one stockholder in the corporation owns 10 percent or more of its stock, of any class, or no individual partner in the partnership owns a 10 percent or greater interest therein, or no member in the limited liability company owns a 10 percent or greater interest therein, as the case may be. **(SKIP TO PART IV)**

(Please attach additional sheets if more space is needed):

Name of Individual or Business Entity	Home Address (for Individuals) or Business Address

Part III DISCLOSURE OF 10% OR GREATER OWNERSHIP IN THE STOCKHOLDERS, PARTNERS OR LLC MEMBERS LISTED IN PART II

If a bidder has a direct or indirect parent entity which is publicly traded, and any person holds a 10 percent or greater beneficial interest in the publicly traded parent entity as of the last annual federal Security and Exchange Commission (SEC) or foreign equivalent filing, ownership disclosure can be met by providing links to the website(s) containing the last annual filing(s) with the federal Securities and Exchange Commission (or foreign equivalent) that contain the name and address of each person holding a 10% or greater beneficial interest in the publicly traded parent entity, along with the relevant page numbers of the filing(s) that contain the information on each such person. **Attach additional sheets if more space is needed.**

Website (URL) containing the last annual SEC (or foreign equivalent) filing	Page #'s

Please list the names and addresses of each stockholder, partner or member owning a 10 percent or greater interest in any corresponding corporation, partnership and/or limited liability company (LLC) listed in Part II **other than for any publicly traded parent entities referenced above.** The disclosure shall be continued until names and addresses of every noncorporate stockholder, and individual partner, and member exceeding the 10 percent ownership criteria established pursuant to N.J.S.A. 52:25-24.2 has been listed. **Attach additional sheets if more space is needed.**

Stockholder/Partner/Member and Corresponding Entity Listed in Part II	Home Address (for Individuals) or Business Address

Part IV Certification

I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder/proposer; that the **<name of contracting unit>** is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with **<type of contracting unit>** to notify the **<type of contracting unit>** in writing of any changes to the information contained herein; 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 am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the, permitting the **<type of contracting unit>** to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print):	Ty Hurner	Title:	CFO
Signature:	<i>Ty Hurner</i>	Date:	11/20/20

DOC #2

NON-COLLUSION AFFIDAVIT

STANDARD BID DOCUMENT REFERENCE	
	Reference: VII-H
Name of Form:	NON-COLLUSION AFFIDAVIT
Statutory Reference:	No specific statutory reference State Statutory Reference N.J.S.A. 52:34-15
Instructions Reference:	Statutory and Other Requirements VII-H
Description:	The Owner's use of this form is optional. It is used to ensure that the bidder has not participated in any collusion with any other bidder or Owner representative or otherwise taken any action in restraint of free and competitive bidding.

NON-COLLUSION AFFIDAVIT

State of New Jersey
County of _____

ss:

I, _____ residing in _____
(name of affiant) (name of municipality)
in the County of _____ and State of _____ of full
age, being duly sworn according to law on my oath depose and say that:

I am _____ of the firm of _____
(title or position) (name of firm)

_____ the bidder making this Proposal for the bid

entitled _____, and that I executed the said proposal with
(title of bid proposal)
full authority to do so that said bidder 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 named project; and that all statements contained in said proposal and in this
affidavit are true and correct, and made with full knowledge that the _____
_____ relies upon the truth of the statements contained in said Proposal
(name of contracting unit)
and in the statements contained in this affidavit in awarding the contract for the said project.

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
_____.

Subscribed and sworn to

before me this day

Signature

_____, 2 _____

(Type or print name of affiant under signature)

Notary public of

My Commission expires _____

(Seal)

**AFFIRMATIVE ACTION AFFIDAVIT
(P.L. 1975, C.127)**

Company Name: Spirion, LLC
Street: 200 Central Ave Ste 1900
City, State, Zip Code: St Petersburg FL, 33701

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.

11/20/20
Date

Ty Hurner
Authorized Signature and Title

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 its 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

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.

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.”

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 Executive}

County Clerk

Surrogate

Sheriff

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.**

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:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:

Subscribed and sworn before me this ___ day of _____, 2__.	_____
(Notary Public)	(Affiant)
My Commission expires:	_____
	(Print name & title of affiant)
	(Corporate Seal)

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.

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.

<https://www.njportal.com/DOR/BusinessRegistration/>

EEOAA EVIDENCE

Equal Employment Opportunity/Affirmative Action
Goods, Professional Services & General Service Projects

EEO/AA Evidence

Vendors are required to submit evidence of compliance with N.J.S.A. 10:5-31 et seq. and N.J.A.C. 17:27 in order to be considered a responsible vendor.

One of the following must be included with submission:

- Copy of Letter of Federal Approval
- Certificate of Employee Information Report
- Fully Executed Form AA302
- Fully Executed EEO-1 Report

See the guidelines at: http://www.state.nj.us/treasury/contract_compliance/pdf/pa.pdf for further information.

I certify that my bid package includes the required evidence per the above list and State website.

Name: Ty Hurner Title: CFO

Signature: *Ty Hurner* Date: 11/20/20

STATE OF NEW JERSEY
Division of Purchase & Property
Contract Compliance Audit Unit
EEO Monitoring Program

EMPLOYEE INFORMATION REPORT

IMPORTANT-READ INSTRUCTIONS CAREFULLY BEFORE COMPLETING FORM. FAILURE TO PROPERLY COMPLETE THE ENTIRE FORM AND TO SUBMIT THE REQUIRED \$150.00 FEE MAY DELAY ISSUANCE OF YOUR CERTIFICATE. DO NOT SUBMIT EEO-1 REPORT FOR SECTION B, ITEM 11. For Instructions on completing the form, go to: https://www.state.nj.us/treasury/contract_compliance/documents/pdf/forms/aa302ins.pdf

SECTION A - COMPANY IDENTIFICATION

1. FID. NO. OR SOCIAL SECURITY 13-4183707	2. TYPE OF BUSINESS <input type="checkbox"/> 1. MFG <input type="checkbox"/> 2. SERVICE <input type="checkbox"/> 3. WHOLESALE <input type="checkbox"/> 4. RETAIL <input checked="" type="checkbox"/> 5. OTHER	3. TOTAL NO. EMPLOYEES IN THE ENTIRE COMPANY 140
4. COMPANY NAME Spirion LLC		
5. STREET 200 Central Ave Ste 1900	CITY St Petersburg	COUNTY Pinellas
		STATE FL
		ZIP CODE 33701
6. NAME OF PARENT OR AFFILIATED COMPANY (IF NONE, SO INDICATE) CITY STATE ZIP CODE		
7. CHECK ONE: IS THE COMPANY: <input checked="" type="checkbox"/> SINGLE-ESTABLISHMENT EMPLOYER <input type="checkbox"/> MULTI-ESTABLISHMENT EMPLOYER		
8. IF MULTI-ESTABLISHMENT EMPLOYER, STATE THE NUMBER OF ESTABLISHMENTS IN NJ		
9. TOTAL NUMBER OF EMPLOYEES AT ESTABLISHMENT WHICH HAS BEEN AWARDED THE CONTRACT		140
10. PUBLIC AGENCY AWARDED CONTRACT CITY COUNTY STATE ZIP CODE		

Official Use Only	DATE RECEIVED	INAUG. DATE	ASSIGNED CERTIFICATION NUMBER

SECTION B - EMPLOYMENT DATA

11. Report all permanent, temporary and part-time employees ON YOUR OWN PAYROLL. Enter the appropriate figures on all lines and in all columns. Where there are no employees in a particular category, enter a zero. Include ALL employees, not just those in minority/non-minority categories, in columns 1, 2, & 3. **DO NOT SUBMIT AN EEO-1 REPORT.**

JOB CATEGORIES	ALL EMPLOYEES			PERMANENT MINORITY/NON-MINORITY EMPLOYEE BREAKDOWN									
	COL. 1 TOTAL (Cols. 2 & 3)	COL. 2 MALE	COL. 3 FEMALE	***** MALE *****					***** FEMALE *****				
				BLACK	HISPANIC	AMER. INDIAN	ASIAN	NON MIN.	BLACK	HISPANIC	AMER. INDIAN	ASIAN	NON MIN.
Officials/ Managers													
Professionals													
Technicians	1	1	0	0	0	0	1	0	0	0	0	0	0
Sales Workers													
Office & Clerical													
Craftworkers (Skilled)													
Operatives (Semi-skilled)													
Laborers (Unskilled)													
Service Workers													
TOTAL	1	1	0	0	0	0	1	0	0	0	0	0	0
Total employment From previous Report (if any)													
Temporary & Part-Time Employees	The data below shall NOT be included in the figures for the appropriate categories above.												

12. HOW WAS INFORMATION AS TO RACE OR ETHNIC GROUP IN SECTION B OBTAINED? <input type="checkbox"/> 1. Visual Survey <input checked="" type="checkbox"/> 2. Employment Record <input type="checkbox"/> 3. Other (Specify)	14. IS THIS THE FIRST Employee Information Report Submitted? 1. YES <input checked="" type="checkbox"/> 2. NO <input type="checkbox"/>	15. IF NO, DATE LAST REPORT SUBMITTED MO. DAY YEAR
13. DATES OF PAYROLL PERIOD USED From: 11/01/2020 To: 11/15/2020		

SECTION C - SIGNATURE AND IDENTIFICATION

16. NAME OF PERSON COMPLETING FORM (Print or Type) McCullough Buchanan	SIGNATURE <i>Cully Buchanan</i>	TITLE DHR	DATE MO DAY YEAR 11 23 2020
17. ADDRESS NO. & STREET 200 Central Ave Ste 1900	CITY St Petersburg	COUNTY Pinellas	STATE FL
		ZIP CODE 33701	PHONE (AREA CODE, NO., EXTENSION) 727 - 440 - 5717

DOC #9
MCBRIDE-PRINCIPLES



STATE OF NEW JERSEY DEPARTMENT OF THE TREASURY
DIVISION OF PURCHASE AND PROPERTY

33 WEST STATE STREET, P.O. BOX 230
TRENTON, NEW JERSEY 08625-0230

MACBRIDE PRINCIPALS FORM

BID SOLICITATION #: _____

VENDOR/BIDDER: _____

VENDOR'S/BIDDER'S REQUIREMENT
TO PROVIDE A CERTIFICATION IN COMPLIANCE WITH THE MACBRIDE PRINCIPALS
AND NORTHERN IRELAND ACT OF 1989

Pursuant to Public Law 1995, c. 134, a responsible Vendor/Bidder selected, after public bidding, by the Director of the Division of Purchase and Property, pursuant to N.J.S.A. 52:34-12, must complete the certification below by checking one of the two options listed below and signing where indicated. If a Vendor/Bidder that would otherwise be awarded a purchase, contract or agreement does not complete the certification, then the Director may determine, in accordance with applicable law and rules, that it is in the best interest of the State to award the purchase, contract or agreement to another Vendor/Bidder that has completed the certification and has submitted a bid within five (5) percent of the most advantageous bid. If the Director finds contractors to be in violation of the principals that are the subject of this law, he/she shall take such 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.

I, the undersigned, on behalf the Vendor/Bidder, certify pursuant to N.J.S.A. 52:34-12.2 that:

CHECK THE APPROPRIATE BOX

The Vendor/Bidder has no business operations in Northern Ireland; or

OR

The Vendor/Bidder will take lawful steps in good faith to conduct any business operations it has in Northern Ireland in accordance with the MacBride principals of nondiscrimination in employment as set forth in section 2 of P.L. 1987, c. 177 (N.J.S.A. 52:18A-89.5) and in conformance with the United Kingdom's Fair Employment (Northern Ireland) Act of 1989, and permit independent monitoring of its compliance with those principals.

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor/Bidder, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor/Bidder is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I will be subject to criminal prosecution under the law, and it will constitute a material breach of **my** agreement(s) with the State, permitting the State to declare any contract(s) resulting from this certification to be void and unenforceable.

Ty Hurner

Signature

11/20/20

Date

Ty Hurner

Print Name and Title