UNIVERSITY
OF
CALIFORNIA

Purchasing Agreement # 2021003169

As a result of Request for Proposal # 002295-DEC2020 UC System-wide Fitness Equipment, the Agreement to furnish certain goods and 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 cooperation ("UC") on behalf of the University of California and the supplier named below ("Supplier"). This Agreement is binding only if it is negotiated and executed by an authorized representative with the proper delegation of authority.

1. Statement of Work

Supplier agrees to perform the Services listed in the statement of work attached as Attachment A ("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.

Cooperative Purchasing: Supplier agrees to extend Goods and/or Services to public agencies (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") registered with OMNIA Partners, Public Sector ("Participating Public Agencies") under the terms of this agreement. All contractual administration (e.g. terms, conditions, extensions, and renewals) will remain the UC's responsibility except as outlined in the above referenced RFP (title of RFP). Operational issues, fiduciary responsibility, payment issues and liabilities, and disputes involving individual Participating Public Agencies will be addressed, administered, and resolved by each Participating Public Agency.

Order of Precedence: Should any conflict arise between the terms of this Agreement and language set forth in the RFP or attachments, the inconsistency shall be resolved by giving precedence in the following order:

1. This agreement – UC wide Fitness and Exercise Solutions 2021003169
2. RFP # - 002295-DEC2020 UC System-wide Fitness Equipment

2. Term of Agreement/Termination

a) The term of the Agreement will be from **November 23, 2021** and through **November 22, 2026** and is subject to earlier termination as provided below. It may be extended upon the agreement of the parties.

b) 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.

c) Notwithstanding anything herein to the contract, neither party may terminate the Agreement or any subsequent PO, once Supplier has ordered the Goods from its manufacturer unless the University makes payment in full for the Goods and/or Services purchased pursuant to the PO.

3. Purchase Order; Advance Payments

Unless otherwise provided in the Agreement, Supplier may not begin providing Goods and/or Services until UC approves a Purchase Order for the Goods and/or Services.

4. Pricing, Invoicing Method, and Settlement Method and Terms

Refer to Attachment A - Statement of Work, Attachment B – Price List or Purchase Order for Pricing. Fitness and Exercise Solutions under the current agreement will provide a 45% discount off MSRP for products listed on Attachment B.

For system-wide agreements, each UC Location will specify the Invoicing Method and Payment Options that will apply, taking into account the operational capabilities of Supplier and the UC Location. See UC's Procure to Pay Standards http://www.ucop.edu/procurement-services/_files/Matrix%20for%20website.pdf for the options that will be considered. In the case of system-wide agreements, each UC Location will specify these terms in a Statement of Work or Purchase Order, as the case may be.

The parties acknowledge and agree Supplier may increase the MSRP prices for the Goods and/or Services as a result of a change in the labor market, material costs, fuel costs, or other related expenses. Supplier shall furnish UC written documentation evidencing the price increase. Any such price increase shall become effective upon thirty (30) days from the date Supplier provided UC with written notice of the price increase.

5. Notices

As provided in the UC Terms and Conditions of Purchase, notices may be given by email, which will be considered legal notice only 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]. If a physical format notice is required, it must be sent by overnight delivery or by certified mail with return receipt requested, at the addresses specified below.

To UC, regarding contract issues:

Name	Sean Parker
Phone	805-451-1545
Email	Sean.Parker@ucop.edu
Address	1111 Franklin St.
	Oakland, CA 94607

To Supplier:

Name	Scott Gilles
Phone	812-455-5241
Email	sgilles@fitexsolutions.com
Address	4610 B Covert Ave, Evansville, IN 47714

6. Intellectual Property, Copyright and Patents

/___/ The Goods and/or Services involve Work Made for Hire

/_X_/ The Goods and/or Services **do not** involve Work Made for Hire

7. Patient Protection and Affordable Care Act (PPACA)

/___/ Because the Services involve temporary or supplementary staffing, they are subject to the PPACA warranties in the T&Cs.

/_X_/ The Services do not involve temporary or supplementary staffing, and they are not subject to the PPACA warranties in the T&Cs.

8. Prevailing Wages

/_X_/ Supplier is not required to pay prevailing wages when providing the Services.

9. Fair Wage/Fair Work

/_X_/ Supplier is not required to pay 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) when providing the Services.

10. Federally Funded Contracts, Grants, and Cooperative Agreements

Not Applicable

11. Restriction Relating to Consulting Services or Similar Contracts – Follow-on Contracts

Please note a Supplier that is awarded a consulting services or similar contract cannot later submit a bid or be considered for any work "required, suggested, or otherwise deemed appropriate" as the end product of the Services (*see* Public Contract Code Section 10515).

12. Insurance

Deliver the PDF version of the Certificate of Insurance to UC's Buyer, by email with the following text in the Subject field: CERTIFICATE OF INSURANCE – **Fitness and Exercise Solutions**

13. Service-Specific and/or Goods-Specific Provisions

Not Applicable

14. Records about Individuals

Records created pursuant to the Agreement that contain personal information about individuals (including statements made by or about individuals) may become subject to the California Information Practices Act of 1977, which includes a right of access by the subject individual. While ownership of confidential or personal information about individuals is subject to negotiated agreement between UC and Supplier, records will normally become UC's property, and subject to state law and UC policies governing privacy and access to files. When collecting the information, Supplier must inform the individual that the record is being made, and the purpose of the record. Use of recording devices in discussions with employees is permitted only as specified in the Statement of Work.

15. Amendments to UC Terms and Conditions of Purchase

Article 2 – Term and Termination

Section C – Revised as follows:

"Either party may, by thirty (30) days prior written notice stating the extent and effective date thereof, terminate the Agreement for convenience in whole or in part, at any time. Notwithstanding anything herein to the contrary, if a party terminates the Agreement once Supplier has ordered the Goods from its manufacturer and is unable to cancel the order with the manufacturer, UC agrees to make payment in full for the Goods and/or Services purchased pursuant to the PO." 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. Except as stated herein, 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."

Section D – Revised to read the following:

"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 twenty (20) business days, or fails to supply the Goods and/or Services within the time specified or any written extension thereof. "

Article 3 – Pricing, Invoicing Method, and Settlement Method and Terms - Revised to read the following:

"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 pay shipping, delivery and handling/installation expenses in accordance with the terms of this Agreement. Every quote and/or subsequent purchase order will have a line item addressing shipping and installation service costs prior to the execution of a purchase order. Unless otherwise agreed upon by the parties in writing, shipping and delivery is to be provided FOB destination. For purposes of this Agreement "FOB destination" shall mean "risk of loss and damage to the Goods shall be Supplier's responsibility until the Goods are delivered to UC's named destination." The parties acknowledge and agree Supplier shall have a third parties provide the shipping and delivery services and handling/installation services at UC's named destination. Thereafter, Supplier shall invoice UC for said shipping, delivery, and handling/installation services, and UC shall pay for said shipping, delivery, and handling/installation services in accordance with this Section.

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 – Revised to read the following:

"The Goods and/or Services furnished will be exactly as specified in the Agreement, free from all defects in 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 by providing written notice to Supplier within five (5) business days from the date of delivery. Thereafter, the Supplier and UC shall, in good faith, work together to submit the claim to the manufacturer of the Goods and request the manufacturer of the Goods to correct them. If the manufacturer is unable or refuses to correct such deficiencies within a reasonable time, UC may terminate the Agreement in whole or in part. Notwithstanding final acceptance and payment, Supplier will be liable for fraud or such gross mistakes as amount to fraud and Supplier shall work with UC in good faith to resolve any claim of liability."

Article 6 – Warranties

Section A – Revised to read as follows:

"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. There are no oral promises, representations or warranties collateral to or affecting this Agreement. The warranties stated herein do not cover wear and tear, overloading, abuse or misuse by UC, its employees, agents or customers, or any other buyer, nor are said warranties applicable in cases where UC or any other buyer has failed to follow instructions supplied by Supplier, nor in case of any defect due to materials, designs or specifications provided to Supplier by UC. NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, THE PARTIES ACKNOWLEDGE AND AGREE ANY WARRANTY RELATED TO THE GOODS SHALL BE PROVIDED BY THE MANUFACTURER OF THE GOODS AND NOT SUPPLIER. AS SUCH, ANY AND ALL WARRANTIES RELATED TO THE GOODS ARE AS SET FORTH IN THE ATTACHED EXHIBIT “A” AND MADE APART HEREOF, AS AMENDED FROM TIME TO TIME BY THE MANUFACTURER. SUPPLIER’S ONLY RESPONSIBILITY AND LIABILITY FOR DEFECTIVE GOODS OR SERVICES SHALL BE TO ASSIST UC OR ANY OTHER BUYER UNDER THIS AGREEMENT WITH FILING A WARRANTY CLAIM WITH THE MANUFACTURER OF THE GOODS. SUPPLIER ACKNOWLEDGES AND AGREES TO WORK WITH UC IN GOOD FAITH TO PROCESS THE WARRANTY CLAIM. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, SUPPLIER MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE OR USE WITH RESPECT TO THE PRODUCTS.”

Section B – Revised to read as follows:

“Permits and Licenses. Supplier agrees to ensure all necessary permits or licenses are obtained 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.”

Section D – Removed in its entirety

Section E – Removed in its entirety

Section F – Removed in its entirety

Article 7 – Intellectual Property, Copyright, Patents and Data Rights

Section A – Revised to read as follows:

a. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, THE GOODS AND DELIVERABLES PROVIDED HEREIN ARE NOT “WORK MADE FOR HIRE” AND UC SHALL NOT ACQUIRE ANY INTELLECTUAL PROPERTY OR LICENSE IN ANY RESPECT THERETO.

b. The Deliverables must be new and original, unless otherwise agreed upon by the parties.

Section B – Revised to read as follows:

a. The Deliverables must be new and original., unless otherwise agreed upon in writing by both parties. Supplier must not use any Pre-Existing Materials in the Deliverables without UC’s prior written permission.

Article 8 – Indemnity and Liability – Revised to read as follows:

“To the fullest extent permitted by law, Supplier will defend, indemnify, and hold harmless UC, its officers, employees, and agents, from and against all third party losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities resulting from or arising out of the Agreement, including the negligent 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 negligent 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. Notwithstanding anything herein to the contrary, Supplier shall not be responsible for defending, indemnifying, and holding UC, its officers, employees, and agents harmless in relation to the negligence of UC, or its officers, employees, and agents. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, SUPPLIER’S TOTAL LIABILITY FOR ANY LOSS, EXPENSE, DAMAGE, OR LIABILITY RELATED

TO AN INDEMNIFICATION OBLIGATION, OR A BREACH OF THIS AGREEMENT OR A BREACH OF ANY WARRANTY, EXPRESS OR IMPLIED, OR ANY OTHER CAUSE, INCLUDING BUT NOT LIMITED TO NEGLIGENCE, SHALL BE LIMITED TO AN AMOUNT EQUAL TO THE LESSER OF: (A) $500,000.00; OR (B) THE TOTAL DOLLAR AMOUNT PAID TO SUPPLIER DURING THE TWELVE (12)-MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION IN THE AGGREGATE."

Article 9 – Insurance

Section F removed in its entirety

Section H revised to read: "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."

Section I revised to read: "The coverages referred to under A and B of this Article must include UC as an additional insured. 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 15 – Liability for UC – Furnished Property

First line will read as follows: "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 reasonable satisfaction."

Article 17 – Additional Terms Applicable to the Furnishing of Goods

A. Price Decreases – Price Decreases. Supplier agrees to notify UC of any price decreases from its suppliers, and provided Supplier's profit margins are not affected, shall pass through to UC any price decreases.

Article 35 – Governing Law and Venue – Revised to read as follows:

"California law will control the Agreement and any document to which it is appended to the extent the Services and Goods are being supplied in California. The exclusive jurisdiction and venue for any and all actions arising out of or brought under the Agreement is in a federal 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. To the extent the Goods or Services are being supplied in a state outside of California, the governing law shall be the State in which the Services are being performed, not including the choice of law rules thereof."

Article 39 – Contracting for Covered Services

Paragraphs 2 and 3 removed. Following language added: "Notwithstanding anything in this Agreement to the contrary, UC acknowledges and agrees that the Services provided by Supplier are not Covered Services.

Exhibit A – Product Warranty Matrix added to the end of the Terms and Conditions

16. Incorporated Documents

This Agreement and its Incorporated Documents contain the entire agreement between the Parties, in order of the below precedent, concerning its subject matter and shall supersede all prior or other agreements, oral and written declarations of intent and other legal arrangements (whether binding or non-binding) made by the Parties in respect thereof.

a. UC wide Fitness and Exercise Solutions 2021003169 Purchasing Agreement
b. UC Terms and Conditions of Purchase (Revised) – dated 4-5-2021
c. Attachment A - Statement of Work Template
d. Attachment B – Fitness and Exercise Solutions Price List
e. UC Request for Proposal # 002295-DEC2020 UC System-wide Fitness Equipment
f. Supplier's responses thereto submitted on or about April 15th 2021 ("RFP Response")
g. UC Sustainable Practices Policy
h. UC HECVAT Form – Optional Campus Specific Form

17. 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.

This Agreement can only be signed by an authorized representative with the proper delegation of authority.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

DocuSigned by:
Sean Parker
55BDE1B322C54AF...
(Signature)

Sean Parker
Acting Associate Director - Strategic Sourcing
(Printed Name, Title)

12/1/2021
(Date)

Fitness and Exercise Solutions, LLC

DocuSigned by:
Scott Gilles
FAA7C87AEC4B4FD...
(Signature)

Scott Gilles owner
(Printed Name, Title)

11/22/2021
(Date)

UNIVERSITY
OF
CALIFORNIA

Terms and Conditions of Purchase

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. Either party may, by thirty (30) days prior written notice stating the extent and effective date thereof, terminate the Agreement for convenience in whole or in part, at any time. Notwithstanding anything herein to the contrary, if a party terminates the Agreement, once Supplier has ordered the Goods from its manufacturer and is unable to cancel the order with the manufacturer, UC agrees to make payment in full for the Goods and/or Services purchased pursuant to the PO. 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. Except as stated herein, 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 twenty (20) business days, or fails to supply the Goods and/or Services within the time specified or any written extension thereof.

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

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 pay shipping, delivery and handling/installation expenses in accordance with the terms of this Agreement. Every quote and/or subsequent purchase order will have a line item addressing shipping and installation service costs prior to the execution of a purchase order. Unless otherwise agreed upon by the parties in writing, shipping and delivery is to be provided FOB destination. For purposes of this Agreement "FOB destination" shall mean "risk of loss and damage to the Goods shall be Supplier's responsibility until the Goods are delivered to UC's named destination." The parties acknowledge and agree Supplier shall have a third parties provide the shipping and delivery services and handling/installation services at UC's named destination. Thereafter, Supplier shall invoice UC for said shipping, delivery, and handling/installation services, and UC shall pay for said shipping, delivery, and handling/installation services in accordance with this Section.

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 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 by providing written notice to Supplier within five (5) business days from the date of delivery. Thereafter, the Supplier and UC shall, in good faith, work together to submit the claim to the manufacturer of the Goods and request the manufacturer of the Goods to correct them. If the manufacturer is unable or refuses to correct such deficiencies within a reasonable time, UC may terminate the Agreement in whole or in part. Notwithstanding final acceptance and payment, Supplier will be liable for fraud or such gross mistakes as amount to fraud and Supplier shall work with UC in good faith to resolve any claim of liability.

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, except for the obligations to pay for any outstanding Services performed or Goods provided.

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.

   There are no oral promises, representations or warranties collateral to or affecting this Agreement. The warranties stated herein do not cover wear and tear, overloading, abuse or misuse by UC, its employees, agents or customers, or any other buyer, nor are said warranties applicable in cases where UC or any other buyer has failed to follow instructions supplied by Supplier, nor in case of any defect due to materials, designs or specifications provided to Supplier by UC. NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, THE PARTIES ACKNOWLEDGE AND AGREE ANY WARRANTY RELATED TO THE GOODS SHALL BE PROVIDED BY THE MANUFACTURER OF THE GOODS AND NOT SUPPLIER. AS SUCH, ANY AND ALL WARRANTIES RELATED TO THE GOODS ARE AS SET FORTH IN THE ATTACHED EXHIBIT "A" AND MADE APART HEREOF, AS AMENDED FROM TIME TO TIME BY THE MANUFACTURER. SUPPLIER'S ONLY RESPONSIBILITY AND LIABILITY FOR DEFECTIVE GOODS OR SERVICES SHALL BE TO ASSIST UC OR ANY OTHER BUYER UNDER THIS AGREEMENT WITH FILING A WARRANTY CLAIM WITH THE MANUFACTURER OF THE GOODS. SUPPLIER ACKNOWLEDGES AND AGREES TO WORK WITH UC IN GOOD FAITH TO PROCESS THE WARRANTY CLAIM. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, SUPPLIER MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE OR USE WITH RESPECT TO THE PRODUCTS.

B. Permits and Licenses. Supplier agrees to ensure all necessary permits or licenses are obtained 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 (Materiel 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. N/A
E. General Accessibility Requirements. N/A
F. Warranty of Quiet Enjoyment. N/A
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. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, THE GOODS AND DELIVERABLES PROVIDED HEREIN ARE NOT "WORK MADE FOR HIRE" AND UC SHALL NOT ACQUIRE ANY INTELLECTUAL PROPERTY OR LICENSE IN ANY RESPECT THERETO.
   b. The Deliverables must be new and original, unless otherwise agreed upon by the parties.
B. Goods and/or Services Not Involving Work Made for Hire.
   a. The Deliverables must be new and original, unless otherwise agreed upon by the parties. Supplier must not use any Pre-Existing Materials in the Deliverables without UC's prior written

permission.

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 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) contact the manufacturer of the Goods and demand that said manufacturer 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, except to pay Supplier for any Services performed and Goods supplied.

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 third party losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities resulting from or arising out of the Agreement, including the negligent 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 negligent 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. Notwithstanding anything herein to the contrary, Supplier shall not be responsible for defending, indemnifying, and holding UC, its officers, employees, and agents harmless in relation to the negligence of UC, or its officers, employees, and agents. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, SUPPLIER'S TOTAL LIABILITY FOR ANY LOSS, EXPENSE, DAMAGE, OR LIABILITY RELATED TO AN INDEMNIFICATION OBLIGATION, OR A BREACH OF THIS AGREEMENT OR A BREACH OF ANY WARRANTY, EXPRESS OR IMPLIED, OR ANY OTHER CAUSE, INCLUDING BUT NOT LIMITED TO NEGLIGENCE, SHALL BE LIMITED TO AN AMOUNT EQUAL TO THE LESSER OF: (A) $500,000.00; OR (B) THE TOTAL DOLLAR AMOUNT PAID TO SUPPLIER DURING THE SIX (6)-MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION IN

THE AGGREGATE.

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. N/A

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. 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. 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.

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 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 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 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 reasonable 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 to notify UC of any price decreases from its suppliers, and provided Supplier's profit margins are not affected, shall 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 30 days prior 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 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

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.);
      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.

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
   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 apprenticable 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 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/fwfw-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/fwfw-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/fwfw-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

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 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

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 to the extent the Services and Goods are being supplied in California. The exclusive jurisdiction and venue for any and all actions arising out of or brought under the Agreement is in a federal 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. To the extent the Goods or Services are being supplied in a state outside of California, the governing law shall be the State in which the Services are being performed, not including the choice of law rules thereof.

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.

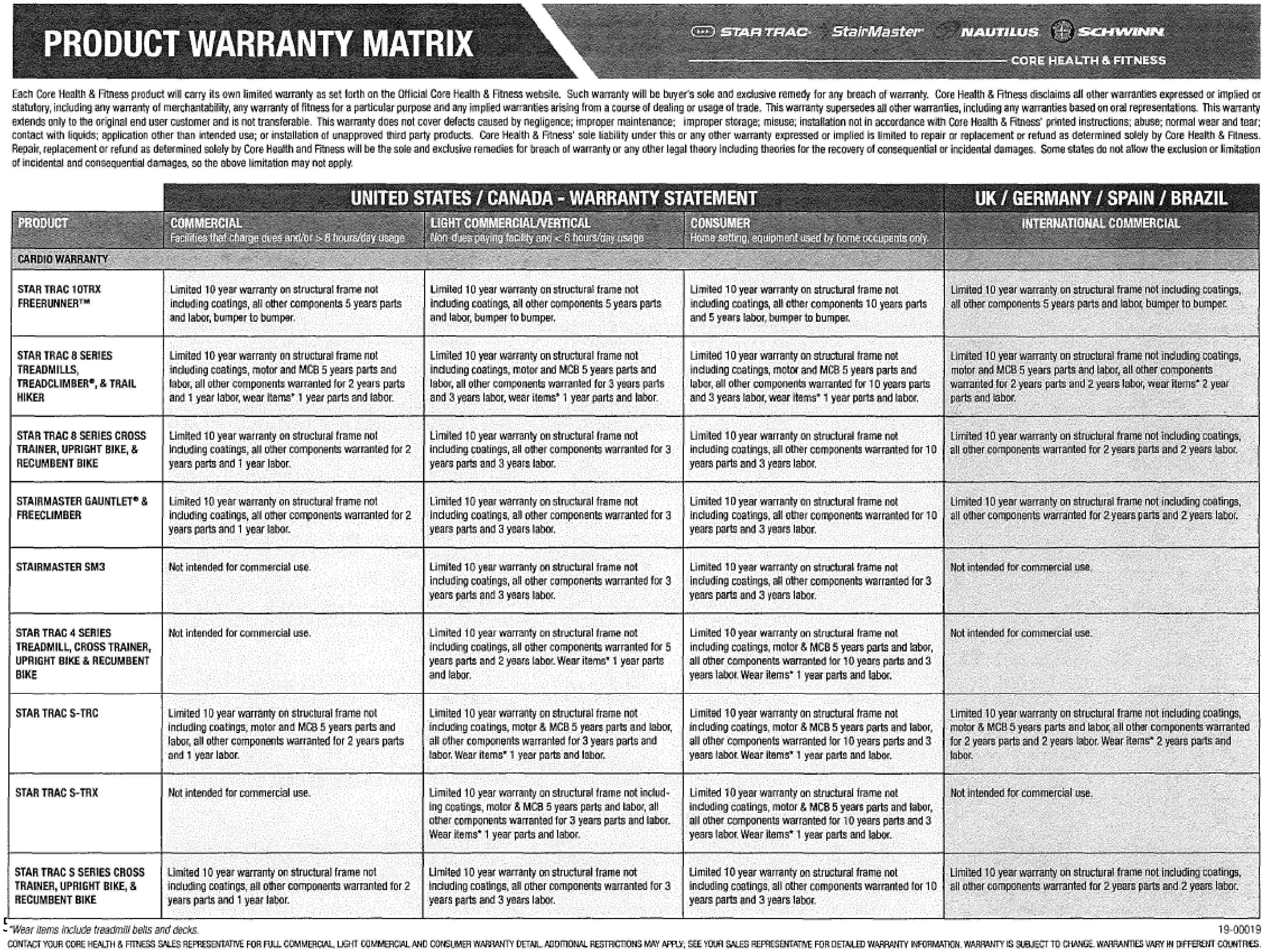
ARTICLE 37 – SUPPLIER TERMS
Any additional terms that Supplier includes in an order form or similar document will be of no force and effect, unless UC expressly agrees in writing to such terms.

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.

Notwithstanding anything in this Agreement to the contrary, UC acknowledges and agrees that the Services provided by Supplier are not Covered Services.

EXHIBIT "A" TO THE UNIVERSITY OF CALIFORNIA TERMS AND CONDITIONS OF PURCHASE



PRODUCT WARRANTY MATRIX

STAR TRAC StairMaster NAUTILUS SCHWINN

CORE HEALTH & FITNESS

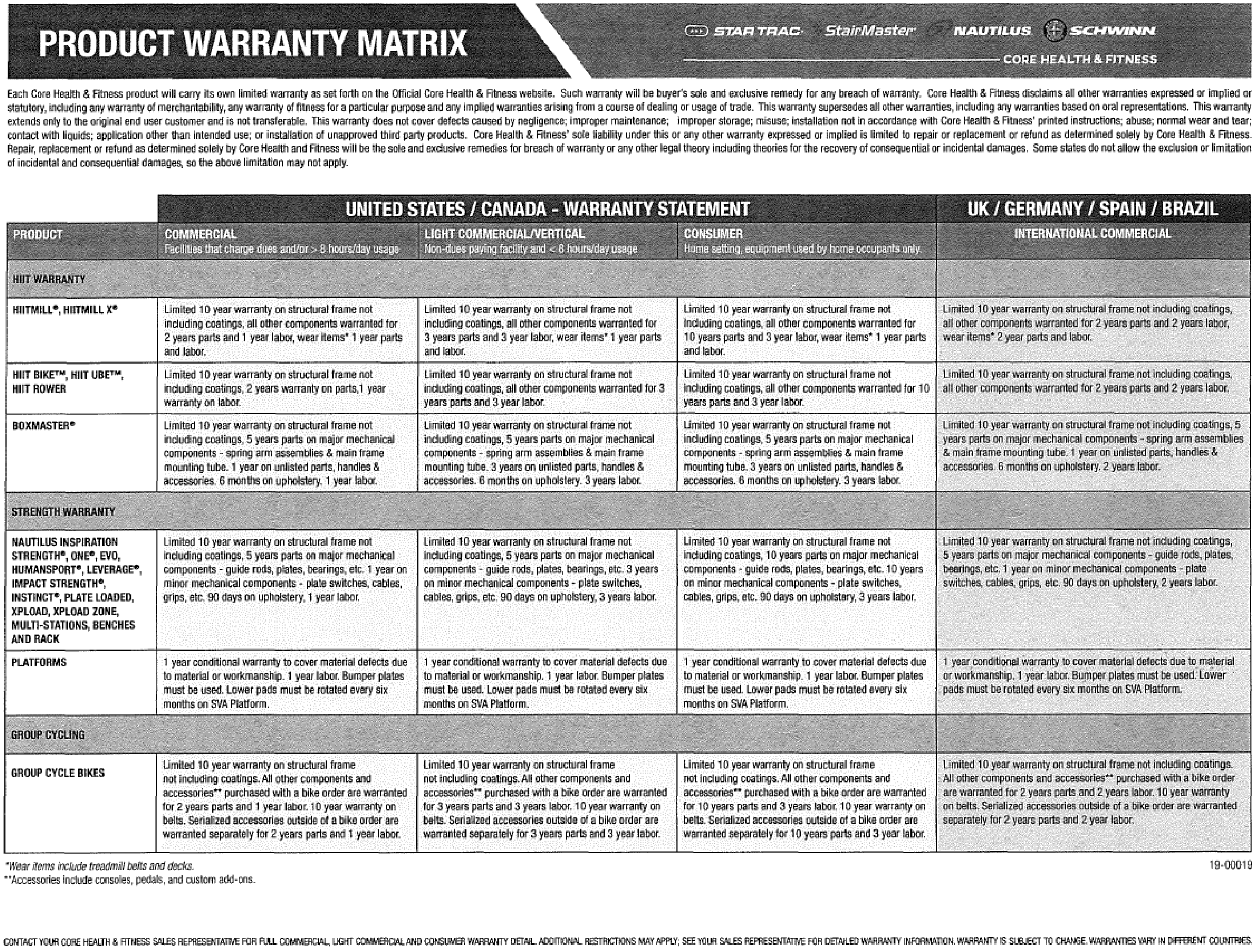
Each Core Health & Fitness product will carry its own limited warranty as set forth on the Official Core Health & Fitness website. Such warranty will be buyer's sole and exclusive remedy for any breach of warranty. Core Health & Fitness disclaims all other warranties expressed or implied or statutory, including any warranty of merchantability, any warranty of fitness for a particular purpose and any implied warranties arising from a course of dealing or usage of trade. This warranty supersedes all other warranties, including any warranties based on oral representations. This warranty extends only to the original end user customer and is not transferable. This warranty does not cover defects caused by negligence; improper maintenance; improper storage; misuse; installation not in accordance with Core Health & Fitness' printed instructions; abuse; normal wear and tear; contact with liquids; application other than intended use; or installation of unapproved third party products. Core Health & Fitness' sole liability under this or any other warranty expressed or implied is limited to repair or replacement or refund as determined solely by Core Health & Fitness. Repair, replacement or refund as determined solely by Core Health and Fitness will be the sole and exclusive remedies for breach of warranty or any other legal theory including theories for the recovery of consequential or incidental damages. Some states do not allow the exclusion or limitation of incidental and consequential damages, so the above limitation may not apply.

	UNITED STATES / CANADA - WARRANTY STATEMENT			UK / GERMANY / SPAIN / BRAZIL
PRODUCT	COMMERCIAL Facilities that charge dues and/or > 8 hours/day usage	LIGHT COMMERCIAL/VERTICAL Non-dues paying facility and < 8 hours/day usage	CONSUMER Home setting, equipment used by home occupants only.	INTERNATIONAL COMMERCIAL
CARDIO WARRANTY				
STAR TRAC 10TRX FREERUNNER™	Limited 10 year warranty on structural frame not including coatings, all other components 5 years parts and labor, bumper to bumper.	Limited 10 year warranty on structural frame not including coatings, all other components 5 years parts and labor, bumper to bumper.	Limited 10 year warranty on structural frame not including coatings, all other components 10 years parts and 5 years labor, bumper to bumper.	Limited 10 year warranty on structural frame not including coatings, all other components 5 years parts and labor, bumper to bumper.
STAR TRAC 8 SERIES TREADMILLS, TREADCLIMBER®, & TRAIL HIKER	Limited 10 year warranty on structural frame not including coatings, motor and MCB 5 years parts and labor, all other components warranted for 2 years parts and 1 year labor, wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, motor and MCB 5 years parts and labor, all other components warranted for 3 years parts and 3 years labor, wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, motor and MCB 5 years parts and labor, all other components warranted for 10 years parts and 3 years labor, wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, motor and MCB 5 years parts and labor, all other components warranted for 2 years parts and 2 years labor, wear items* 2 year parts and labor.
STAR TRAC 8 SERIES CROSS TRAINER, UPRIGHT BIKE, & RECUMBENT BIKE	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 1 year labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 3 years parts and 3 years labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 10 years parts and 3 years labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 2 years labor.
STAIRMASTER GAUNTLET® & FREECLIMBER	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 1 year labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 3 years parts and 3 years labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 10 years parts and 3 years labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 2 years labor.
STAIRMASTER SM3	Not intended for commercial use.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 3 years parts and 3 years labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 3 years parts and 3 years labor.	Not intended for commercial use.
STAR TRAC 4 SERIES TREADMILL, CROSS TRAINER, UPRIGHT BIKE & RECUMBENT BIKE	Not intended for commercial use.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 5 years parts and 2 years labor. Wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, motor & MCB 5 years parts and labor, all other components warranted for 10 years parts and 3 years labor. Wear items* 1 year parts and labor.	Not intended for commercial use.
STAR TRAC S-TRC	Limited 10 year warranty on structural frame not including coatings, motor and MCB 5 years parts and labor, all other components warranted for 2 years parts and 1 year labor.	Limited 10 year warranty on structural frame not including coatings, motor & MCB 5 years parts and labor, all other components warranted for 3 years parts and labor. Wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, motor & MCB 5 years parts and labor, all other components warranted for 10 years parts and 3 years labor. Wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, motor & MCB 5 years parts and labor, all other components warranted for 2 years parts and 2 years labor. Wear items* 2 years parts and labor.
STAR TRAC S-TRX	Not intended for commercial use.	Limited 10 year warranty on structural frame not including coatings, motor & MCB 5 years parts and labor, all other components warranted for 3 years parts and labor. Wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, motor & MCB 5 years parts and labor, all other components warranted for 10 years parts and 3 years labor. Wear items* 1 year parts and labor.	Not intended for commercial use.
STAR TRAC S SERIES CROSS TRAINER, UPRIGHT BIKE, & RECUMBENT BIKE	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 1 year labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 3 years parts and 3 years labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 10 years parts and 3 years labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 2 years labor.

*Wear items include treadmill belts and decks.

19-00019

CONTACT YOUR CORE HEALTH & FITNESS SALES REPRESENTATIVE FOR FULL COMMERCIAL, LIGHT COMMERCIAL AND CONSUMER WARRANTY DETAIL. ADDITIONAL RESTRICTIONS MAY APPLY; SEE YOUR SALES REPRESENTATIVE FOR DETAILED WARRANTY INFORMATION. WARRANTY IS SUBJECT TO CHANGE. WARRANTIES VARY IN DIFFERENT COUNTRIES.



PRODUCT WARRANTY MATRIX

STAR TRAC StairMaster NAUTILUS SCHWINN

CORE HEALTH & FITNESS

Each Core Health & Fitness product will carry its own limited warranty as set forth on the Official Core Health & Fitness website. Such warranty will be buyer's sole and exclusive remedy for any breach of warranty. Core Health & Fitness disclaims all other warranties expressed or implied or statutory, including any warranty of merchantability, any warranty of fitness for a particular purpose and any implied warranties arising from a course of dealing or usage of trade. This warranty supersedes all other warranties, including any warranties based on oral representations. This warranty extends only to the original end user customer and is not transferable. This warranty does not cover defects caused by negligence; improper maintenance; improper storage; misuse; installation not in accordance with Core Health & Fitness' printed instructions; abuse; normal wear and tear; contact with liquids; application other than intended use; or installation of unapproved third party products. Core Health & Fitness' sole liability under this or any other warranty expressed or implied is limited to repair or replacement or refund as determined solely by Core Health & Fitness. Repair, replacement or refund as determined solely by Core Health and Fitness will be the sole and exclusive remedies for breach of warranty or any other legal theory including theories for the recovery of consequential or incidental damages. Some states do not allow the exclusion or limitation of incidental and consequential damages, so the above limitation may not apply.

	UNITED STATES / CANADA - WARRANTY STATEMENT			UK / GERMANY / SPAIN / BRAZIL
PRODUCT	COMMERCIAL Facilities that charge dues and/or > 8 hours/day usage	LIGHT COMMERCIAL/VERTICAL Non-dues paying facility and < 8 hours/day usage	CONSUMER Home setting, equipment used by home occupants only.	INTERNATIONAL COMMERCIAL
HIIT WARRANTY				
HIITMILL®, HIITMILL X®	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 1 year labor, wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 3 years parts and 3 year labor, wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not Including coatings, all other components warranted for 10 years parts and 3 year labor, wear items* 1 year parts and labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 2 years labor, wear items* 2 year parts and labor.
HIIT BIKE™, HIIT UBE™, HIIT ROWER	Limited 10 year warranty on structural frame not including coatings, 2 years warranty on parts,1 year warranty on labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 3 years parts and 3 year labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 10 years parts and 3 year labor.	Limited 10 year warranty on structural frame not including coatings, all other components warranted for 2 years parts and 2 years labor.
BOXMASTER®	Limited 10 year warranty on structural frame not including coatings, 5 years parts on major mechanical components - spring arm assemblies & main frame mounting tube. 1 year on unlisted parts, handles & accessories. 6 months on upholstery. 1 year labor.	Limited 10 year warranty on structural frame not including coatings, 5 years parts on major mechanical components - spring arm assemblies & main frame mounting tube. 3 years on unlisted parts, handles & accessories. 6 months on upholstery. 3 years labor.	Limited 10 year warranty on structural frame not including coatings, 5 years parts on major mechanical components - spring arm assemblies & main frame mounting tube. 3 years on unlisted parts, handles & accessories. 6 months on upholstery. 3 years labor.	Limited 10 year warranty on structural frame not including coatings, 5 years parts on major mechanical components - spring arm assemblies & main frame mounting tube. 1 year on unlisted parts, handles & accessories. 6 months on upholstery. 2 years labor.
STRENGTH WARRANTY				
NAUTILUS INSPIRATION STRENGTH®, ONE®, EVO, HUMANSPORT®, LEVERAGE®, IMPACT STRENGTH®, INSTINCT®, PLATE LOADED, XPLOAD, XPLOAD ZONE, MULTI-STATIONS, BENCHES AND RACK	Limited 10 year warranty on structural frame not including coatings, 5 years parts on major mechanical components - guide rods, plates, bearings, etc. 1 year on minor mechanical components - plate switches, cables, grips, etc. 90 days on upholstery, 1 year labor.	Limited 10 year warranty on structural frame not including coatings, 5 years parts on major mechanical components - guide rods, plates, bearings, etc. 3 years on minor mechanical components - plate switches, cables, grips, etc. 90 days on upholstery, 3 years labor.	Limited 10 year warranty on structural frame not including coatings, 10 years parts on major mechanical components - guide rods, plates, bearings, etc. 10 years on minor mechanical components - plate switches, cables, grips, etc. 90 days on upholstery, 3 years labor.	Limited 10 year warranty on structural frame not including coatings, 5 years parts on major mechanical components - guide rods, plates, bearings, etc. 1 year on minor mechanical components - plate switches, cables, grips, etc. 90 days on upholstery, 2 years labor.
PLATFORMS	1 year conditional warranty to cover material defects due to material or workmanship. 1 year labor. Bumper plates must be used. Lower pads must be rotated every six months on SVA Platform.	1 year conditional warranty to cover material defects due to material or workmanship. 1 year labor. Bumper plates must be used. Lower pads must be rotated every six months on SVA Platform.	1 year conditional warranty to cover material defects due to material or workmanship. 1 year labor. Bumper plates must be used. Lower pads must be rotated every six months on SVA Platform.	1 year conditional warranty to cover material defects due to material or workmanship. 1 year labor. Bumper plates must be used. Lower pads must be rotated every six months on SVA Platform.
GROUP CYCLING				
GROUP CYCLE BIKES	Limited 10 year warranty on structural frame not including coatings. All other components and accessories** purchased with a bike order are warranted for 2 years parts and 1 year labor. 10 year warranty on belts. Serialized accessories outside of a bike order are warranted separately for 2 years parts and 1 year labor.	Limited 10 year warranty on structural frame not including coatings. All other components and accessories** purchased with a bike order are warranted for 3 years parts and 3 years labor. 10 year warranty on belts. Serialized accessories outside of a bike order are warranted separately for 3 years parts and 3 year labor.	Limited 10 year warranty on structural frame not including coatings. All other components and accessories** purchased with a bike order are warranted for 10 years parts and 3 years labor. 10 year warranty on belts. Serialized accessories outside of a bike order are warranted separately for 10 years parts and 3 year labor.	Limited 10 year warranty on structural frame not including coatings. All other components and accessories** purchased with a bike order are warranted for 2 years parts and 2 years labor. 10 year warranty on belts. Serialized accessories outside of a bike order are warranted separately for 2 years parts and 2 year labor.

*Wear items include treadmill belts and decks.

**Accessories include consoles, pedals, and custom add-ons.

19-00019

CONTACT YOUR CORE HEALTH & FITNESS SALES REPRESENTATIVE FOR FULL COMMERCIAL, LIGHT COMMERCIAL AND CONSUMER WARRANTY DETAIL. ADDITIONAL RESTRICTIONS MAY APPLY; SEE YOUR SALES REPRESENTATIVE FOR DETAILED WARRANTY INFORMATION. WARRANTY IS SUBJECT TO CHANGE. WARRANTIES VARY IN DIFFERENT COUNTRIES.

ATTACHMENT A TO PURCHASING AGREEMENT #______

STATEMENT OF WORK

This Statement of Work # __ ("SOW") is issued pursuant to Purchasing Agreement #_______ dated ________________, 20__ between UC and Supplier ("Agreement").

1. Title and Description of the Scope of Goods and/or Services

[Buyer: Provide an overview and background of Goods and/or Services to be provided.]

2. Term of SOW

This SOW will begin on __________, 20__ ("Effective Date") and continue through ______________, 20__. This SOW may not be renewed or otherwise amended except through a Change Order pursuant to the Change Management section below.

3. Key Tasks and Activities, Deliverables and Completion Timeframe

Supplier Obligations				
Task		**Activities**	**Deliverables**	**Completion Date or Timeframe**
1	**[General description]**	**[Specific details using action verbs like "create", "develop", "test", "analyze", "evaluate", etc.]**	**[List each discrete tangible work product that is considered a critical end result from the Supplier; deliverables are nouns, not verbs]**	**[Specific dates are best; can be stated as "Week 1", "Week 2", etc.]**
2				
3				
4				
5				
Additional as needed		**Include: Identify all phases. If additional phases will not be known until first phase work begins, be sure to specify hourly rate and a not to exceed price for this work.** **Request Supplier to provide data type, protected health information and other data**		

4. UC Obligations

[Buyer: Include as appropriate language such as: UC will provide working space, equipment, furniture, utilities, and services, as follows:]

5. Place(s) of Performance

[Buyer: Use this section if appropriate to outline where Services will be provided]

6. Key Personnel

Supplier’s Account Manager is listed below, is subject to UC approval, and has overall responsibility for managing the UC/Supplier relationship:

Name	
Phone	
Email	
Address	

Subcontractors authorized to provide Goods and/or Services under this SOW **[Buyer: Names should be listed only if Agreement permits use of subcontractors]**:

Name of Subcontractor	**Goods and/or Services the Subcontractor will provide**

Supplier’s Account Management Team is:

Name	
Phone	
Email	
Address	
Name	
Phone	
Email	
Address	
Name	
Phone	
Email	
Address	
Name	
Phone	
Email	
Address	

UC’S Project Manager, responsible for acceptance/rejection of project results/deliverables, is:

Name	
Phone	
Email	
Address	

7. Reporting Requirements

[Buyer: Identify any key reports that should be produced by Supplier or critical reporting events. This can be included in the table above if preferred.]

Supplier agrees to provide other reports as reasonably requested by UC during the Term of the Agreement and any extension(s) to the Term at no additional cost to UC.

8. Assumptions

a) The following items are not included within the scope of Goods and/or Services to be provided under this SOW: **[Buyer: Delete if not needed]**

b) **[Buyer: Add more as needed]**

c) Additional assumptions include the following: **[Buyer: Delete if not needed, but list any UC dependencies that must be fulfilled in order for Supplier to provide the Goods and/or Services]**

d) **[Buyer: Add more as needed]**

9. Service Level Agreement

a) **[Buyer: Any critical SLAs should be stated here. For goods, consider the following language:]**

During the Term of the Agreement, and any extension(s) of the Term, Supplier will provide the following minimum service standards:

Normal delivery	-next business day
Rush delivery	-within 4 hours
Pick up returns	-within 2 business days
Request for reports	-within 5 business days
Order fill rate	-98%
Delivery accuracy	-98%
Delivery, on-time	-98%
Invoice/billing accuracy	-98%
Customer service satisfaction	-98%

The minimum service standards set forth above recognize that occasional errors are likely; however, Supplier further agrees to use its best efforts to achieve 100% of service levels. Should the service levels fall below the minimum standards and Supplier does not take corrective action within fourteen (14) days following UC written notification, UC reserves the right to terminate the Agreement immediately.

10. Pricing, Invoicing Method, and Settlement Method and Terms

[Buyer: Pricing includes the contract amount (for instance, time and materials using an hourly rate; whether there is a not to exceed cap; and flat fee); and the payment schedule (what percentage must be paid at what times, including milestones)]

Pricing is addressed below. The Invoicing Method, and Settlement Method and Terms are addressed in the applicable Agreement. As regards Invoicing Method, and Settlement Method and Terms, the terms of the applicable Agreement will take precedence over any conflicting terms in this Statement of Work.

a) "Fixed Price Services" to be rendered under this SOW, including deliverables to be provided as part of Fixed Price Services, are described in this section as:

b) "Time and Materials Services" to be rendered under this SOW, including deliverables to be provided as part of Time and Materials Services:

c) The rates applicable to each person who will render Time and Materials Services are as follows:

Name and Title of Person Rendering Services	**Rate per Hour/Day**	**Estimated No. of Days**	**Extended Cost of Fees**	**UC MRC**
Estimated Maximum Expenses (if any):			**n/a**	

Estimated Maximum Cost:		

d) [Buyer: Outline Payment Schedule as needed]

11. Program Requirements

[Buyer: If items will be ordered by catalog, use the Appendix – Electronic Commerce. If applicable, consider using these additional terms for Goods:]

Order Packaging and Labeling. Supplier agrees that each UC order will be individually wrapped and labeled with the following information:

Purchase Order number;

Product description, quantity and catalog number of the product ordered and an open 30-character field for internal identification e.g., UC storehouse catalog numbers and/or internal customer order numbers; and

Other information, as may be requested by ordering UC Location.

Packaging slips will be attached to the outside of the package such that it can be inspected by UC at the requesting department and/or receiving dock.

Receiving Locations. Supplier agrees to provide desktop and dock delivery to all UC current and future authorized personnel delivery points, as requested by UC.

Standard Delivery Requirements. Supplier will deliver Monday through Friday, excluding UC- and Supplier-observed holidays. Supplier provide UC with a schedule on or before September 1 of the following calendar year showing holidays and other planned shutdowns (such as the annual inventory) that would impact Supplier's ability to deliver the Goods and/or Services. Supplier agrees to deliver all UC orders received by 3:30pm Pacific Time the next business day as follows:

Campus direct (desktop delivery)	- by 3:30 pm Pacific Time
Storehouse (drop ship delivery)	- by 10:00 am Pacific Time

Delivery Delays. Supplier will report any delivery delay whatsoever to the ordering Location, as well as its cause, within two (2) hours after Supplier is able to reasonably determine there will be a delay; the report will be provided to UC by telephone, e-mail, or facsimile. Supplier will keep UC fully informed and will take all reasonable action in eliminating the cause of delay.

Rush Delivery Requirements. Supplier agrees to deliver UC emergency orders within four (4) hours after receipt of order at no additional charge to UC. Rush delivery orders for same day delivery must be requested by UC prior to 1:00 pm Pacific Time. Supplier cannot guarantee, but agrees to use good faith efforts to provide same day delivery for rush orders UC places after 1:00 pm Pacific Time.

Returns. Supplier agrees to accept Goods returned by UC if in resalable condition and if made within thirty (30) days of original shipment. Supplier must pick up returns from the ordering department location within two business days. Services under $20.00 do not need to be physically returned to Supplier.

Credit. Requests for credit can be transmitted by the ordering UC personnel via the established order management system (telephone, fax, paper return form, and web-based). Chargebacks and credit memos will be issued to UC ordering departments in the current month's billing period. Return items will be credited at cost. If Goods were purchased via UC purchasing card, credit must be issued to the same purchasing card.

Out of Stock Items. If there is an out of stock situation of any ordered inventoried item(s), the out of stock item will be added to the back order file and will be delivered to UC when the item is in stock without a further order being submitted.

Surveys. Supplier will, at UC's request, conduct customer surveys of UC orders through questionnaires. The content of these surveys will be approved by UC. UC will be responsible for the tabulation of these surveys.

12. Acceptance Criteria and Testing

[Buyer: Provide details of the Acceptance Criteria and testing which each Deliverable or Milestone must meet to be accepted, if specifics aren't defined.]

a) **[Buyer: Indicate any additional financial or other considerations resulting from acceptance testing]**

13. Changes to the Services

UC may desire to change the Goods and/or Services following execution of an SOW. If so, UC will submit a written Amendment to Supplier describing the changes in appropriate detail. If an Amendment does not require Supplier to incur any additional material costs or expenses, then Supplier will make the modification within ten (10) business days of Supplier's receipt of UC's Amendment. If an Amendment does require that Supplier incur additional material costs or expenses, then Supplier in good faith will provide UC with a written, high level, non-binding assessment of the costs and expenses and the time required to perform the modifications required by the Amendment, within ten (10) business days of Supplier's receipt of UC's Amendment. UC will notify Supplier in writing within ten (10) business days after receipt of Supplier's response to the Amendment as to whether UC wishes Supplier to implement the Amendment based on the response. UC will compensate Supplier for implementation of an Amendment in accordance with the terms and conditions of the relevant Amendment and Supplier's response to the Amendment, if any. Supplier's implementation of an Amendment will not delay the performance of Services and/or the delivery of deliverables not reasonably affected by an Amendment.

14. No Mandatory Use

Because there is no mandatory use policy at UC, nothing in this Statement of Work will be construed to prevent UC from entering into similar agreements with any third parties including, without limitation, suppliers that may be in competition with Supplier.

15. Additional Terms

[Buyer: If recording devices will be allowed, add the following: Supplier will use recording devices in discussions with UC employees only when UC and the employees so authorize; this authorization must be in writing. If applicable, Supplier's use of recording devices in such discussion is proposed as follows: (Insert terms)]

Insurance Requirements **[Buyer: insert terms, if needed or different from basic levels in T&Cs]**

This Statement of Work is signed below by the parties' duly authorized representatives.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA	**[SUPPLIER NAME]**
______________________________ (Signature)	______________________________ (Signature)
______________________________ (Printed Name, Title)	______________________________ (Printed Name, Title)
______________________________ (Date)	______________________________ (Date)

The Regents
of
the University of California

REQUEST FOR PROPOSAL (RFP)

FOR

UC System-wide Fitness Equipment
RFP# 002295-DEC2020
Date Issued: 3/4/2021

It is the Supplier's responsibility to read the entire document, any addendums and to comply with all requirements listed herein. Any addenda to this Request for Proposal will be directed to all participating Suppliers. It is the Suppliers responsibility to watch their e-mail for any addendums, notices, or changes to the RFP or process.

Issued By: The Regents of the University of California

RFP Administrator:
Sean Parker, Acting Associate Director
System-wide Procurement Services
Strategic Sourcing
University of California, Office of the President
1111 Franklin Street, 10th Floor
Oakland, CA 94607-5200

The information contained in this Request for Proposal (RFP) is confidential and proprietary to the University of California and is to be used by the recipient solely for the purpose of responding to this RFP.

TABLE OF CONTENTS

SECTION I: UNIVERSITY OF CALIFORNIA OVERVIEW

A) Background

The University of California ("UC"), one of the largest and most acclaimed institutions of higher learning in the world, is dedicated to excellence in teaching, research, health care and public service. It is a public institution with annual resources of over $34 billion and encompasses ten campuses, six medical schools and five medical centers, four law schools and a statewide Division of Agriculture and Natural Resources. The University is also involved in the operation and management of three national laboratories for the U.S. Department of Energy.

System-wide management of the University of California is assigned to the Office of the President based in Oakland, California. Its divisions oversee UC's academic mission, budget, external relations, legal matters, and business and financial activities (including the UC Office of the Chief Investments Officer). The University is governed by a Board of Regents consisting of 26 members, 18 of whom are appointed by the Governor for 12-year overlapping terms.

Website:	https://www.universityofcalifornia.edu/
Established:	1868
Fiscal Year:	07.01.XX - 06.30.XX
Official incorporated entity:	The Regents of the University of California

B) Recreation and Athletic Operations Summary

Each UC Campus has a combination of athletic training facilities and recreation centers dedicated to sports, recreation, and wellness. In addition to students, faculty and staff also participate in programs at these facilities and centers. It is anticipated that use of these facilities will increase which will in turn demand new equipment, maintenance and regular replacement equipment. These facilities manage large areas housing cardio and strength equipment; they allocate additional space to other disciplines including Pilates, yoga, massage, and group fitness.

Fitness equipment is purchased by UC campuses for:

- Replacement equipment for existing equipment that is older or that has a high failure rate
- Additional equipment for existing facilities
- Equipment for new, remodeled, or auxiliary facilities
- New state of the art equipment for athletic focused departments

The current estimated annual spend of UC fitness equipment products is **$1,200,000.00**

The above figure is provided as an annual estimate only to assist Suppliers in preparing proposals. The figure provided is indicative of the potential business volume and the complexity of the account. ***However, the University does not and cannot guarantee any specific quantities or business volume during the agreement period or any extensions thereto***.

Currently, most UC locations have a Small Business Program in place for purchasing products and services from small and local businesses. The University will continue purchasing through its current Small Business Programs and these efforts are coordinated at the location level.

Most of the location's central receiving docks can accommodate 45 ft. or larger delivery trucks; buildings without loading docks can accommodate 30-ft. and smaller delivery trucks.

SECTION II: INTRODUCTION TO THE REQUEST FOR PROPOSAL

The University of California's overall objective of the RFP is to select a supplier or suppliers to assist UC in establishing the most cost effective and efficient procurement program for fitness equipment while maintaining high standards of quality and service. With that intent UC is interested in evaluating the costs and benefits of dealer and/or manufacturing partnerships for acquisition of fitness equipment focusing on cardio and strength training to UC locations.

This project was initiated to develop a supplier/UC alliance(s) and implement a UC system-wide program for fitness equipment that will provide maximum value to the University through superior equipment, enhanced variety, superior customer service, streamlined processes, maintenance, and lower total costs.

Qualified original equipment dealers and manufacturers are invited to submit proposals, based on the information provided in this RFP, to establish a business partnership with UC which will maximize the resources of both organizations to most effectively meet the fitness equipment needs of the University of California. The resulting awarded contract will consist of one term of five (5) years with the University's option to renew five, one year extensions after the term is successfully completed (10 years total). The successful Supplier(s) shall be required to meet the requirements listed within this solicitation.

Qualified dealers and manufacturers are understood to have met the following requirements:

Dealers:

Previous experience with university/athlete clientele

Manufacturers:

Previous experience with university/athlete clientele, and

Offer a minimum 5 year warranty on parts, services or a combination thereof

National Contract

The University of California, as the Principal Procurement Agency, defined in Exhibit A, has partnered with OMNIA Partners, Public Sector ("OMNIA Partners") to make the resultant contract (also known as the "Master Agreement" in materials distributed by OMNIA Partners) from this solicitation available to other public agencies nationally, including state and local governmental entities, public and private primary, secondary and higher education entities, non-profit entities, and agencies for the public benefit ("Public Agencies"), through OMNIA Partners' cooperative purchasing program. The University of California is acting as the contracting agency for any other Public Agency that elects to utilize the resulting Master Agreement. Use of the Master Agreement by any Public Agency is preceded by their registration with OMNIA Partners (a "Participating Public Agency") 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 a Master Intergovernmental Cooperative Purchasing Agreement, a form of which is attached hereto on Exhibit C, or as otherwise agreed to. Exhibit A contains additional information about OMNIA Partners and the cooperative purchasing program.

OMNIA Partners is the largest and most experienced purchasing organization for public and private sector procurement. Through the economies of scale created by OMNIA Partners public sector subsidiaries and affiliates, National IPA and U.S. Communities, our participants now have access to more competitively solicited and publicly awarded cooperative agreements. The lead agency contracting process continues to be the foundation on which we are founded. OMNIA Partners is proud to offer more value and resources to state and local government, higher education, K-12 education and non-profits.

OMNIA Partners provides shared services and supply chain optimization to government, education and the private sector. With corporate, pricing and sales commitments from the Supplier, OMNIA Partners provides marketing and administrative support for the Supplier that directly promotes the Supplier's products and services to Participating Public Agencies though multiple channels, each designed to promote specific products and services to Public Agencies on a national basis. Participating Public Agencies benefit from pricing based on aggregate spend and the convenience of a contract that has already been advertised and publicly competed. The Supplier benefits from a contract that generally allows Participating Public Agencies to directly purchase goods and services without the Supplier's need to respond to additional competitive solicitations. As such, the Supplier must be able to accommodate a nationwide demand for services and to fulfill obligations as a nationwide Supplier and respond to the OMNIA Partners documents (Exhibit A, B, F, G).

The University of California anticipates spending approximately $12M over the full potential Master Agreement term for UC System-wide Fitness Equipment. While no minimum volume is guaranteed to the Supplier, the estimated annual volume of UC System-wide Fitness Equipment purchased under the Master Agreement through OMNIA Partners is approximately $36M. This projection is based on the current annual volumes among the University of California, other Participating Public Agencies 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 the Supplier and OMNIA Partners.

All products and services are subject to review and approval by the University.

SECTION III: PROPOSAL EVALUATION METHODOLOGY

Responsive Proposals will be evaluated using a Best Value method. Best Value means the most advantageous balance of price/cost, quality, service performance and other elements, as defined by the University. University evaluators will determine the Proposal's value by scoring the Proposals based on a uniform set of weighted evaluation criteria. Each Proposal's Best Value score will be the average of all evaluators' total scores awarded for the Proposal. The University will have determined the Maximum Possible Price Score prior to the Proposal due date. The Proposal with the Maximum Possible Price Score will be considered the lowest responsive Proposal.

All other responsive Proposals will receive a proportion of the Maximum Possible Price Score equal to the quotient of the lowest Proposal's cost divided by that Proposal's cost. Each Proposal's Price Score will be added to that Proposal's Quality Point Score to get that Proposal's Total Score. The Proposal with the highest Total Score will be considered the "Best Value". The Proposal with the next highest Total Score will be considered the second Best Value, and so on. The University will then determine if the Supplier submitting the Best Value Proposal is responsible. The apparent RFP winner(s) will be the responsible Supplier(s) submitting the Best Value Proposal. The University's selection may be made on the basis of the initial Proposals or the University may elect to negotiate with Suppliers who are selected as finalists. The Evaluation Team may utilize Supplier's Oral Presentations, software demonstrations, additional material information, or References from the Supplier and others to come to a determination of award(s).

The University reserves the right to make evaluation decisions at its sole discretion. In performing its review of proposals, the University reserves the right to obtain and use in its evaluation any independently derived information including, but not limited to, financial reports and secondary customer references.

Right to Cancel/Modify

The University reserves the right to change any aspect of, terminate, or delay this RFP, the RFP process and/or the program outlined within this RFP at any time. Notice shall be provided in a timely manner thereafter. The University may award the contract without further discussion or may enter into negotiations with the apparent RFP winner. Should the apparent RFP winner fail to accept the award, the University may determine that that Supplier has abandoned its Proposal. The University may then enter into negotiations with the responsible Supplier submitting the second Best Value Proposal. If that Supplier fails to accept the award, the University may determine that that Supplier has abandoned its Proposal and enter into negotiations with the responsible Supplier submitting the third Best Value Proposal and so on to each successive responsible Best Value Supplier until an award is made and accepted. The University may also conduct concurrent negotiations with responsible Suppliers for the purpose of altering or otherwise changing the conditions, terms and price of the proposed contract unless prohibited. Suppliers shall be accorded fair and equal treatment in conducting negotiations and there shall be no disclosure of any information derived from proposals submitted by competing Suppliers.

Right to Make No Award

The University reserves the right to reject all Proposals and to make no award. Unless stated otherwise in this RFP, the University reserves the right to make multiple awards or to award items separately or in the aggregate as the interests of University may appear.

Minimum Criteria

Proposals will be screened as to whether the following minimum qualifications are met:

- The proposal must be submitted on time.
- The proposal includes all requested documents and has fully answered all required questions.
- Respondents must meet the following minimum criteria:
    - DEALERS:
        - Previous experience with university/athlete clientele with references
    - MANUFACTURERS:
        - Previous experience with university/athlete clientele with references
        - Offer a minimum 5 year warranty on parts, services or a combination thereof

Evaluation Criteria

Qualification measurements may include, but are not limited to the following:

Dual Category Weighting (Dealer vs. Manufacturer)

Dealer Questionnaire Weighting

Section	Weight
Company Information and Capabilities	10%
Sustainability	15%
Product Overview	35%
Services, Training and Warranties	10%
Pricing – Dealer Specific	30%

Manufacturer Questionnaire Weighting

Section	Weight
Company Information and Capabilities	10%
Sustainability	15%
Product Overview	20%
Services, Training and Warranties	20%
Pricing –Manufacturer Specific	35%

Proposal Acceptance

Proposal must be complete and comply with all specifications and legal requirements set in this Request for Proposal.

The University reserves the right to reject any submittals which are:

- Incomplete or non-responsive
- Late (late proposals are immediately rejected)

If, at any time, it is found that a person, firm or corporation in their response to this RFP, or to which an Agreement has been awarded, has colluded with any other party or parties, the University reserves the right to reject the proposal(s) and/or terminate any Agreement(s) so awarded and all parties involved in the collusion shall be liable to the University for all loss or damages which the University may have suffered.

SECTION IV: RFP SCHEDULE

Event	*Date
RFP Issue Date	**3/4/2021 at 5:00PM PST**
Supplier RFP Zoom Call **Email Sean.Parker@ucop.edu for details**	**3/18/2021 at 11:00AM PST**
Supplier RFP Questions Deadline in CalUSource	**3/24/2021 by 5:00PM PST**
UC Response to Supplier Questions (distributed to all Suppliers without attribution on CalUSource)	**3/31/2021**
RFP Responses Due	**4/15/2021 by 5:00PM PST**
Anticipated Award Date	6/15/2021
Anticipated Start Date	6/16/2021

The University does not guarantee the above schedule and reserves the right to modify this schedule at its discretion. ****Please mark off calendars**

**The UC reserves the right to conduct interviews with some or all of the Supplier's at any point during the evaluation process. While presentations are anticipated for this project, the UC may determine interviews are not necessary. In the even interviews or presentations are conducted, information provided during the interview/presentation process shall be taken into consideration when evaluating the stated criteria. The UC shall not reimburse the Supplier for the costs associated with the interview process.

SECTION V: SUPPLIER REQUIREMENTS

The requirements shown below are essential to the UC for proposal consideration. Supplier's failure to provide or be in compliance with any one or more of the following requirements will negatively impact the evaluation of Suppliers proposal and may result in disqualification. All required documents must be accepted before Suppliers can submit proposals on the CalUSource platform.

While this section may reflect the needs and requirements of the UC, OMNIA Partners Participating Public Agencies may have different requirements. The awarded Supplier(s) may enter into a supplemental agreement with Participating Public Agencies (PPAs) and PPAs may elect to negotiate certain terms to conform to their purchasing and contracting requirements.

a) The University of California Terms and Conditions of Purchase, dated 2/27/20, as referenced in ***Guidelines to this RFP***, will be incorporated into any Agreement that may result from this RFP.

b) The University of California Appendix – Data Security and Privacy, dated 8/12/19, as referenced in ***Guidelines to this RFP***, will be incorporated into any Agreement that may result from this RFP.

c) HECVAT example documentation and process acknowledgement

d) All proposals shall remain available for UC acceptance for a minimum of 180 days following the RFP close date.

e) While Successful Supplier(s) awarded a national contract shall be required to sign the UC's Master Agreement and OMNIA Partners Administration Agreement, if Respondents have any additional or separate Service Agreements that they would require the UC or Participating Public Agencies to sign, Respondents shall provide those Service Agreements as part of their response. See the referenced question in the Company Information Questionnaire.

f) No late proposals will be accepted. Any proposals received after the specified deadline for submission shall result in automatic disqualification.

SECTION VI: GENERAL INFORMATION

A. Issuing Office and Communications Regarding the RFP

This RFP, and any subsequent addenda to it, is being issued by the System-wide Procurement Services Department on behalf of The University of California Office of the President. The System-wide Procurement Services Department is the sole point of contact regarding all procurement and contractual matters relating to the requirements described in this RFP. System-wide Procurement Services is also the only office authorized to change, modify, clarify, etc., the specifications, terms, and conditions of this RFP and any Agreements(s) awarded as a result of this RFP.

Any requests for clarification concerning this RFP must be submitted via the CalUSource platform, under the Discussion Forum icon 💬.

The submission of RFP response, pricing proposal and attachments must be submitted via the CalUsource e-Sourcing application, as further detailed in the *"Instructions for Submitting Proposals"* below.

Suppliers are advised that failure to adhere to the above communications requirements may result in disqualification.

B. Supplier RFP Zoom Call

Suppliers are welcome to join a **Supplier RFP Zoom call hosted on Thursday, March 18th 2021, at 11:00am PST.** Please email Sean.Parker@ucop.edu for details and a log in link. This call will review the function of the CalUSource platform and how to submit proposals. While the purpose of this conference will be to clarify the CalUSource platform utilization, any content questions for this Request for Proposal shall be submitted via the process described below. Oral statements or instructions on the call will not constitute an Addendum to this Request for Proposal.

C. Instructions for Submitting Proposals

Proposals in response to this RFP must be submitted online using the CalUsource e-Sourcing application **no later than April 15th, 2021 at 5:00 p.m. (PT).**

Please review the CalUSource Resource Guide for any questions regarding operation of the RFP platform and submitting proposals.

Suppliers are to complete the questionnaire sections directly in the CalUSource e-Sourcing application.

******CalUsource requires significant time for accurate data entry. Suppliers are encouraged to review the Resource Guide and familiarize themselves with the process of responding, leaving adequate time to submit the proposal. General information and support is available by email: support@ucprocure.zendesk.com; or, for CalUsource technical issues, contact GEP Support: 1-732-428-1578 or support@gep.com. Please identify yourself as registering in the University of California network.******

Suppliers must provide a complete, straightforward, concise response to all prerequisites, questions and information in the RFP as detailed. **Do not reference previous answers as the submission for questions (i.e. "Please see response to question 5a").** Submission of a proposal via the CalUsource e-Sourcing application confirms Supplier's understanding and acceptance of all requirements, terms, and conditions of the RFP.

Supplier must not provide superfluous materials such as marketing materials or website links in response to, or in lieu of, specific responses to the questions herein, and may be disqualified for providing superfluous materials.

D. Addenda to the Request for Proposal

Any changes, additions, or deletions to this RFP will be in the form of written Addenda issued by the University of California via email or the CalUsource e-Sourcing application. The University will not be responsible for failure of any prospective Supplier to receive such Addenda. All Addenda so issued shall become part of this RFP.

E. Supplier Questions

An opportunity to submit questions will be allowed up to **5pm (PT), March 31st, 2021.**

Note: All Supplier questions will be shared with all RFP participants, without attribution, on the CalUSource platform under the Discussion Forum icon 💬. Email responses will not be provided.

F. Proposal Acceptance

The proposal must be completed and submitted via the CalUSource e-Sourcing application on the forms provided or in the format indicated herein.

All documents submitted to the UC on behalf of this RFP will become the exclusive property of the UC system and will not be returned.

G. Proposal Format

Proposals should demonstrate a clear understanding of the Scope of Services and contain a comprehensive discussion of how the Supplier will fulfill the requirements of the Scope of Services, including a discussion of the important features and Supplier attributes, highlighting any aspects, which separate it from its competitors. The UC reserves the right to make additional investigations as it deems necessary to establish the competence and financial stability of any Supplier submitting a proposal. Additionally, to comprehensively evaluate the proposals received, the UC may seek additional information or clarification from one or more of the Suppliers. Experience with the UC and entities that evaluation committee members represent may be taken into consideration when evaluating qualifications and experiences. The proposal should be submitted using the appropriate response templates provided on CalUSource:

1. Company Information Questions
2. Sustainability Questions
3. Product Overview
4. Services, Training and Warranty Offerings
5. Pricing (Dealer or Manufacturer)

H. Proposal Preparation Costs

Supplier will bear all costs incurred in the preparation and submission of the Proposal and related documentation, including Supplier's presentation to UC. If Supplier is apparent awardee, Supplier will bear its own costs in negotiating and finalizing an agreement with the University.

I. Agreement Term

It is anticipated that the initial term of any Agreement awarded pursuant to this RFP will be for a period of five (5) years. UC may, at its option, extend or renew the Agreement for five additional one-year periods on the same terms and conditions. As previously stated, the successful Supplier(s) shall also have the right to enter local "service" agreements with Participating Public Agencies accessing the contract through OMNIA Partners, so long as the effective date of such agreement is prior to the expiration of the Contract. All local agreements may have a full potential term (any combination of initial and renewal periods) not to exceed ten (10) years. Any purchase orders executed against this Master Agreement during the effective term may survive beyond the expiration of the Master Agreement as established and agreed to by both parties.

SECTION VII: SCOPE OF SERVICES

Deliverables: Suppliers are to provide responses in the RFP under the following questionnaire categories. The following categories focus on key points in a partnership between a supplier and the UC around fitness equipment purchases and ownership opportunities.

I. Company Information Questions:

Suppliers shall submit responses with information covering general firm structure, financial records, locations for California and national coverage, previous experience and client references.

As detailed in the Company Information Questionnaire, Respondents are to provide a detailed response to Exhibit A, OMNIA Partners Response for National Cooperative contract which will be utilized in the evaluation process to access the national capabilities of Respondents.

II. Sustainability Questions:

Responses to the sustainability questionnaire should focus on the firm, its processes and products through a sustainability lens. These include employment strategies, business certifications, and operations within the company.

III. Product Overview Questions:

Successful Supplier(s) shall provide products focused on cardio and strength training equipment utilized in recreational and/or high performing athletic gyms. This section covers product offerings, product details, replacement parts and customization.

IV. Services, Training and Warranties Questions:

Suppliers are asked to detail their service, training and warranty options available to the UC or a Participating Public Agency. Questions focus on available resources for service, education, warranty terms and logistics.

V. Pricing:

The successful Supplier(s) shall provide a complete set of pricing information for the products under the categories “Cardio Equipment” and/or “Strength Training Equipment”. These pricing questions are broken into two modules focused on Dealer or Manufacturer business structures. The pricing schedule supplied shall reflect “National” pricing, regardless of participating campuses or participating Public Agencies. The prices quoted in the proposal response by the successful Supplier(s) shall be the UC net price for the various services/materials. For items in the bid pricing submitted, there shall be no separate or additional charges, fees, handling or other incidental costs following contract award; Participating Public Agencies may make exceptions to this based on their own circumstances.

Special Offers/Promotions

In addition to decreasing prices for the balance of the Contract term due to a change in market conditions, Contractor may conduct sales promotions involving price reductions for a specified lesser period. Contractor may offer Participating Agencies competitive pricing which is lower than the not-to-exceed price set forth herein at any time during the Contract term and such lower pricing shall not be applied as a global price reduction under the Contract.

Product Offering/Balance of Line Pricing

Pricing for complete product offering/balance of line items will be determined by a percentage discount off retail. The pricing percentage discount offered must be entered in the Pricing section of the Supplier's response.

SECTION VIII: QUESTIONNAIRE(S)

Refer to the CalUsource e-Sourcing application to complete the Questionnaire section(s) of the proposal.

There are five (5) questionnaire categories that need to be completed in total. **Dealers and Manufacturers, please select and submit the pricing module questionnaire that best reflects your firm's designation.**

1. Company Information Questions
2. Sustainability Questions
3. Product Overview Questions
4. Services, Training and Warranty Offerings
5. FOR MANUFACTURERS – Pricing
   FOR DEALERS – Pricing

All questions must be answered as part of the proposal. If the response requires an attachment (do not submit sales brochures), add the attachments in the question directly or the Attachment Section of the CalUsource eSourcing tool and reference the question number in the title of the document.

Suppliers shall respond to the aforementioned questionnaires in order to be considered for evaluation. Failure to answer the following questions could result in disqualification.

SECTION IX: ATTACHMENTS

1. UC Terms and Conditions of Purchase dated 2-27-20
2. UC Required Supplier Information dated 8-5-19
3. UC Appendix Data Security and Privacy dated 4-12-19
4. HECVAT Example Documents
5. Supplier Bidding Guide for CalUSource
6. _Omnia Partners – Exhibit Descriptions for CalUSource
7. Omnia Partners - Exhibit A - Response for National Cooperative Contract
8. Omnia Partners - Exhibit B – Administration Agreement Example
9. Omnia Partners - Exhibits C – Master Intergovernmental Cooperative Purchasing Agreement Example
10. Omnia Partners - Exhibit D – Principal Procurement Agency Certificate Example
11. Omnia Partners - Exhibit E – Contract Sales Reporting Template
12. Omnia Partners - Exhibit F – Federal Funds Certifications Form
13. Omnia Partners - Exhibit G – New Jersey Compliance Form
14. Omnia Partners - Exhibit H – Advertising Compliance Requirement

002295-Dec2020 - Fitness Equipment RFP - UC System-wide

Questionnaire Name:*	Company Information
Questionnaire Type:	Commercial
Questionnaire Description:	General company information

SECTION NAME	QUESTION NUMBER	QUESTION TITLE	QUESTION WEIGHT	RESPONSE OPTIONS	Fitness and Exercise Solutions LLC
General Company Information	1	* Full name; Legal and Trade Name	-	-	Fitness and Exercise Solutions LLC
General Company Information	2	* Authorized Negotiator (name and email address of person(s) in your organization authorized to negotiate contract terms and render binding decisions on contract matters)	-	-	Kelsi Carnes
General Company Information	3	* Address	-	-	4610 B Covert Ave
General Company Information	4	* Phone Number & Fax Number	-	-	615-390-5078
General Company Information	5	* Website Address	-	-	www.fitexsolutions.com
General Company Information	6	* Parent Company (if operating as a subsidiary or affiliate)	-	-	NA
General Company Information	7	* Indicate Entity Type; partnership, corporation, individual, etc.	-	-	Partnership
General Company Information	8	* Public or Private Company	-	-	Private
General Company Information	9	* Date Company Founded	-	-	05/2011
General Company Information	10	* State of Incorporation or Formation	-	-	Indiana
General Company Information	11	* List of branch offices or other subordinate elements that will perform or assist in performing work herein	-	-	NA
General Company Information	12	* Do you intend to use subcontractors? If yes, provide the name, address, and phone number of any subcontractor that you will obtain via contract to perform any portion of work proposed in this RFP.	-	-	No
General Company Information	13	Do you require background checks of subcontractors? What training do you provide to these subcontractors?	-	-	NA
Operational Company Information	14	* Do you outsource any administrative services to a third-party provider? If so, provide details.	-	-	No
Operational Company Information	15	* Submit audited financial statements for the past two (2) years in order to establish financial viability.	-	-	Attached 2019 and 2020 PNL Statements **Attached Files :** FES PNL EOY 2020.pdf;FES PNL EOY 2019.pdf
Operational Company Information	16	* Provide your organization's Dun and Bradstreet (DUNS) number.	-	-	026684771
Operational Company Information	17	* Has your organization experienced recent merger or acquisition activity, or has any such pending activity been publicly disclosed? If so, describe, specifically addressing any reorganization or operational changes that would affect your product or services.	-	-	No
Operational Company Information	18	* Are there any recent or anticipated changes in your organizational structure (e.g. key personnel, consolidation of operations, new service centers) that would impact UC. Include a project plan and timeline if applicable.	-	-	No
Operational Company Information	19	* Is any litigation pending against your organization? If so, give details.	-	-	No
Operational Company Information	20	* Has your company ever filed for bankruptcy? If so, when and what is the current status of your filing?	-	-	No
Operational Company Information	21	* Provide the following information relative to your current Book of Business: A.) Total Clients B.) Total Clients with similar size as the UC	25.00%	-	Our current list of clients includes 2,750 independent customers. Our largest customers include the YMCA of Greater Indianapolis, the University of Tennessee.
Operational Company Information	22	* Describe your company experience with customers in Higher Education and/or academic medical centers. Please also reference your experience with Power 5, collegiate athletics programs.	25.00%	-	FES has a long history of providing products and services to many Power 5 colleges within our region. Throughout the years, we have successfully completed projects for Indiana University, the University of Kentucky, Purdue University and the University of Tennessee. Our current and past service clients include the University of Louisville, Ohio State University, Notre Dame University and Vanderbilt University. These schools, along with many other non-Power 5 D1 and D2 schools, have equipped us with a vast amount of experience in catering to the specific needs of collegiate athletes, trainers and coaches.
Operational Company Information	23	* Summarize in 500 words or less the following: why you are a match for UC, how are you a match for other Participating Public Agencies, and why UC should select your organization over your competitors. Emphasize how you are different from your competitors.	25.00%	-	FES is a unique company in that, while we are a much smaller company than some other regional dealers, we have the experience and infrastructure to provide quality products and service to larger customers. In doing this, we're also able to provide specific attention to the University of California's needs. We are a family-owned local business with the same capabilities as larger nationwide dealers, and our strong vendor relationship with Core Health and Fitness and our long history of excellence set us apart.
Operational Company Information	24	* If Supplier is a current or previous UC Service Provider, give the agreement term dates, agreement number, contracting department, services provided and agreement revenue of agreement(s) for the prior five (5) years.	-	-	NA
Operational Company Information	25	* Provide the primary contact information for the person responsible for your proposal. Include name, title, address, phone number, and email address.	-	-	Kelsi Carnes, Sales Representative, 5304 Missionary Way Brentwood, TN 37027, 615-390-5078, kcarnes@fitexsolutions.com
Operational Company Information	26	* Are any of the members of your Board of Directors, officers, employees, or consultants affiliated with UC? If so, describe the relationship. Are any of these individuals responsible, in whole or in part, for the preparation of your proposal or would they have any decision-making role if your company were awarded the bid?	-	-	No
Operational Company Information	27	* Provide three (3) current client references and two (2) terminated client references. Provide the company name, individual name, title and contact information, and the dates the client is/was active. Priority should be given to California clients.	-	-	Current: YMCA of Greater Indianapolis (Kristi Selker; AVP; kselker@indymca.org; 20+ years), Tennessee Tech University (Suzann Hensley; Campus Recreation Director; shensley@tntech.edu; since 2019), Cumberland University (Ron Pavan; Athletic Director; rpavan@cumberland.edu; since 2019). Prior: University of Evansville (Jeff Chestnut; Fitness Director; jc56@evansville.edu; 20+ years - no business since 2017), YMCA Monroe County (Amy Plunkett; Wellness Director; aplunkett@monroecountyymca.org; 15+ years - no business since 2019). **Attached Files :** 1688_001.pdf;Cumberland University.pdf
Operational Company Information	28	* Have you provided a detailed response to the national program (Omnia Exhibit A)? Responses should highlight experience, demonstrate a strong national presence, describe how offeror will educate its national sales force about the contract, describe how products and services will be distributed nationwide, include a plan for marketing the products and services nationwide, and describe how volume will be tracked and reported to OMNIA Partners.	25.00%	Yes;No	No
Operational Company Information	29	* Have you reviewed Omnia Partners Exhibit B? The Successful Supplier(s) will be required to sign Exhibit B, OMNIA Partners Administration Agreement. Suppliers should have any reviews required to sign the document prior to submitting a response. Supplier's response should include any proposed exceptions to the OMNIA Partners Administration Agreement.	-	Yes;No	Yes
Operational Company Information	30	Does your firm have additional or separate Service Agreements that are required for the UC or Participating Public Agencies to sign? If so, please attach those documents for review.	-	-	No

002295-Dec2020 - Fitness Equipment RFP - UC System-wide

Questionnaire Name: *	Sustainability
Questionnaire Type:	Technical
Questionnaire Description:	

SECTION NAME	QUESTION NUMBER	QUESTION TITLE	QUESTION WEIGHT	RESPONSE OPTIONS	Fitness and Exercise Solutions LLC
Company Information	1	Is your company certified in the State of California or other U.S. State as a SBE, DBE, WBE, MBE, VBE, or DVBE? Please submit requisite certification documentation.	5.57%	Small Business Enterprise (SBE); Disadvantaged Business Enterprise (DBE); Women-owned Business Enterprise (WBE); Minority Business Enterprise (MBE); Veteran-owned Business Enterprise (VBE); Disabled Veteran-owned Business Enterprise (DVBE); Other	Small Business Enterprise (SBE)
Company Information	2	Do you have a Corporate Social Responsibility (CSR) statement/policy/code of conduct or equivalent?	5.56%	Yes; No; In Progress	In Progress
Company Information	2.1	If Yes ,Is it publicly available?	N/A	-	
Company Information	2.2	If Yes ,Please provide an information link. If not publicly available, please provide a copy with your response.	N/A	-	
Company Information	3	How do you monitor/manage your supply chain to ensure that suppliers/providers comply with and support your CSR efforts?	5.56%	-	Employees in our receiving/warehouse department are specifically tasked with notifying management in the event they come across any slight or overt occurrence of a vendor or employee committing any act that isn't socially or environmentally conscious. While we cannot necessarily change how our suppliers and vendors conduct business, we are aware and do take notice - alternate supplier Wsources are immediate
Company Information	4	Describe how your company supports its employees by providing living wages and benefits.	5.56%	-	Warehouse and staff employees are provided with wages that meet or exceed the local average for similar work type/employment. Being a smaller family-owned business, we are able to accommodate employee requests that extend beyond the usual sick days/paid vacation standard. Great flexibility is given to assist with employees' personal obligations, whether they be medical, legal or otherwise personal needs.
Company Information	5	Describe your employee healthcare and other benefits provided to your employees.	5.56%	-	Due to our size, we are unable to provide group health insurance to our employees at a rate that would be any more beneficial than the premiums already paid for their individual insurance. To help mitigate this, FES offers assistance in obtaining the most affordable health insurance rates for each individual employee that requests it. We also offer small interest-free loans (for most any reason), and with our close local ties to realtors and investors, we can aggressively seek out and secure the most affordable housing options available for those employees in need.
Company Information	6	Does the company engage only contractors/business partners which adhere to all applicable local, state and federal labor and employment requirements relating to, e.g., wage payment, anti-discrimination/harassment, equal opportunity, family and medical leave, and other applicable provisions?	5.56%	-	Yes - FES ownership has developed a decades-long reputation in the community as fair-dealing individuals, and we make it a point to engage with partners of similar repute.
Company Information	7	Does your company maintain clear diversity goals, such as with regard to women, veterans, and minorities, and engage in active diversity efforts toward recruitment and retention as well as development and advancement? Please provide at least two examples.	5.56%	-	Throughout it's different incarnations, since 1942, FES has never defined any position within the company as gender or race-specific. In all online job postings, we always identify ourselves as a "Second Chance Employer", and offer the same opportunities to anyone, regardless of race, personal gender identification or past criminal history. We have employed female service technicians, male office workers, and African-American sales representatives. Advancement within the company has always been based on ability and enthusias we simply want the "best person for the job", regardless of who the person is, or was.
Company Information	8	Describe in general terms how your company supports your local community and regional businesses and markets. Provide documents, when available, such as your company's economic policies, specific examples outlining past activities, or other information that describes your company's commitment to supporting these economies.	5.56%	-	FES routinely donates to and particpates in sponsorships through local YMCAs, schools and churches.
Company Information	9	What percentage products and services for the company's operation do small and diverse suppliers provide?	5.56%	-	True quality commercial fitness equipment can really only be obtained through large major manufacturers, located all across the country (and the world). That being said, we exclusively rely on longstanding locally-owned outfits to provide us with our operational in-house needs. Building maintenance and repairs, delivery truck servicing and maintenance, and all tools and supplies are locally-sourced to help contribute to our local economy. The mutual trust and strong relationships we've developed between ourselves and local providers, throughout the years, is something we take great pride in.
Company Information	10	Please provide a detailed description of all small and diverse business classifications you track (examples include: Small Business Enterprises, Disadvantaged Business Enterprises, Women-owned Business Enterprises, Service Disabled Veteran-owned Business Enterprises, etc.).	5.56%	-	FES has essentially had the same primary family-based ownership in Evansville, IN for decades, so we do not necessarily track any of these classifications, outside of SBE.
Operations	11	Describe specifically how your company will incorporate environmentally conscious business practices into the delivery of the requested services of this project. Explain how these results will be reported to the UC.	5.56%	-	Our vendor partner, Core Health and Fitness, will be handling the delivery and warranty servicing of all product sold. They share our same focus of corporate-wide environmental responsibility in both their manufacturing process, and product delivery.
Operations	12	Does your company responsibly dispose of old equipment and electronics at the end of its useful life (i.e., through an e-Steward certified recycling partner, self performed recycling measures)?	5.56%	Yes; No	Yes
Operations	13	Describe your company's ability to reduce impacts from travel and meetings as part of service delivery.	5.56%	-	We mainly provide service and delivery to three states (Indiana, Kentucky and Tennessee). We employ only small diesel engine trucks for deliveries, and hybrid fuel passenger vehicles for our service technicians. For cost and environmental reasons, we always deploy only the absolute minimum number of vehicles necessary to complete a job. Eliminating waste is always a priority.
Operations	14	Does your company have a sustainable travel policy that encourages or requires using the lowest impact transport method when multiple options are available?	5.56%	Yes; No	Yes
Operations	15	Does your company have a sustainable travel policy that encourages or requires using public transportation, bicycling, or walking for short-distance trips?	5.56%	Yes; No	Yes
Operations	16	Does your company provide subsidized public transportation options for all employees, as well as incentivize and facilitate employee participation in other alternative forms of work commuting such as membership in bike-shares, free bicycle parking and shower/locker facilities, etc.?	5.56%	-	Being a company that's entrenched in the fitness industry, many of our employees are very health conscious and, as a result, often walk or ride their bikes to work on a regular basis. When possible, car-pooling is encouraged and engaged in. Working from home is an option that is often taken advantage of, for office staff that are able to work remotely.
Operations	17	Is your company an EPA registered SmartWay Partner or Affiliate (https://www.epa.gov/smartway/meet-smartway-partners-and-affiliates), or do you work with companies who are registered? Provide a link certifying your affiliation.	5.56%	-	FES is not currently registered with EPA SmartWay.
Operations	18	The UC has a ban on the procurement of expanded plastic foam materials (such as Expanded Polystyrene (EPS), Expanded Polyethylene (EPE), Expanded Polyurethane and expanded plastic foam hybrids) other than those used for medical or laboratory supply, by 2020. Please describe your company's current utilization of these materials in its packaging, and how your company will assist the University in achieving this goal.	5.56%	-	All of our shipping material is paper-based. When possible, FES re-uses packaging from incoming shipments to package outgoing shipments. No plastic foam material is ever used.

002295-Dec2020 - Fitness Equipment RFP - UC System-wide

Questionnaire Name: *	Product Overview
Questionnaire Type:	Technical
Questionnaire Description:	Questions focused on product offering, specifications, as well as pricing.

SECTION NAME	QUESTION NUMBER	QUESTION TITLE	QUESTION WEIGHT	RESPONSE OPTIONS	Fitness and Exercise Solutions LLC
-	1	Does your firm's experience and offering typically focus on general fitness equipment,high performing athletes or both?	7.14%	Recreation/General Fitness Focus; High Performing Athlete Focus; Both	Both
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category	7.15%	Selectorized - Recreational Equipment	19 (one line)
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Selectorized - High Performing Athlete Equipment	33 (two lines)
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Selectorized - Both	23 (one line)
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category	7.15%	Plate Loaded - Recreational Equipment	0
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Plate Loaded - High Performing Athlete Equipment	0
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Plate Loaded - Both	16
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Free Weight - Recreational Equipment	8
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Free Weight - High Performing Athlete Equipment	19
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Free Weight - Both	17
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Cable - Recreational Equipment	0
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Cable - High Performing Athlete Equipment	0
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Cable - Both	12 (two lines)
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Functional Training Accessories - Recreational Equipment	99+
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Functional Training Accessories - High Performing Athlete Equipment	99+
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Functional Training Accessories - Both	99+
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category	7.15%	Cardio - Recreational Equipment	15
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category	7.15%	Cardio - High Performing Athlete Equipment	36
-	2	Provide a count of equipment models your firm can offer focused around cardio and strength training for recreational gyms,high performing collegiate athletes or both. Please enter quantities for model counts under respective category columnsor the both column.	7.15%	Cardio - Both	12
-	3	Will your firm provide the UC a discount off list or specific pricing per product? (Please provide details in the Pricing Questionnaire)	7.14%	Percentage discount off list; Catalog style, discounted pricing, with	Percentage discount off list
-	4	What gauge steel do your products utilize for strength training equipment?	7.14%	-	7 & 11
-	5	What parts are the most commonly replaced pieces on your equipment?	-	-	Weight Stack Cables and Belts
-	6	What is the lead time for the aforementioned commonly replaced parts?	-	-	One Week
-	7	Are there any product lines in your portfolio that the University should be aware of with upcoming updates or discontinuations?	-	-	No
-	8	What specifications with your product offeringshave provided potential ownership challenges in the past (technological, structural, user experience)?	7.14%	-	Nothing atypical to any commercial fitness manufacturer/product.
-	9	Please designate which ASTM standards your company complies with.	7.14%	-	F1749-15, F2276-10, F2571-15
-	10	Dueto varying campus constraints in the UC system, can all of your equipment offerings be delivered on a box style truck with a lift gate? If not, which products would require a loading dock to be delivered?	7.14%	-	Yes
-	11	For equipment with padding or cushions, how often do those pieces need to be replaced?	7.14%	-	It varies upon usage, but it should not be more often than once every 2-3 years, on average.
-	12	Are your products domestically manufactured?	7.14%	-	A portion of Core's product lineup is manufactured in the United States.
-	13	Which products in your offering are your highest selling units?	7.14%	-	The Stairmaster Gauntlet Stepmills (all models), 10 Series FreeRunner Treadmill and Instinct Duals.
-	14	For those highest selling units, what are their respective life cycles for ownership (in years)?	7.14%	-	Product tends to be traded in within a 5-8 year period, but they are designed to last much longer.
-	15	What recommendations do you have for UC when evaluating similar equipment that your competitors may offer?	-	-	Note the variety between Core's family of products, as opposed to their competitors.
-	16	When technology is present, does your product offering have a remote, over-the-air, software update process? If so, please list which products	7.14%	-	All console software can be updated online, via wired or wireless connection.
-	17	What types of ancillary costs have come up for your clients in your firm's experience around the installation/utilization of your products? (i.e. re-drilling of slab connections, structural modifications, door removal)	7.14%	-	It entirely depends on the customer's facility preferences, but electrical expense is most common.
-	18	What products in your offering are customizable to client needs? Provide a count of models and options that are typically customized	7.14%	-	The 15/19" Cardio consoles have a wide range of customization available - 15 individual units.

002295-Dec2020 - Fitness Equipment RFP - UC System-wide

Questionnaire Name: *	Services, Training and Warranty Offerings
Questionnaire Type:	Commercial
Questionnaire Description:	Questions focused on firm's ability to provide equipment timely, service equipment, offer client training and warranty products.

SECTION NAME	QUESTION NUMBER	QUESTION TITLE	QUESTION WEIGHT	RESPONSE OPTIONS	Fitness and Exercise Solutions LLC
-	1	In confirming a long term partnership with the UC, what is the turnover rate for employees in your company or assigned dealers, both in the sales and service areas?	6.68%	-	For direct employees of the company we have an average turnover rate.
-	2	What product-specific training is offered to your employees or assigned dealers when they begin working with your organization?	-	-	Training involves in-person training, virtual training, and product comprehension testing.
-	3	What product-specific training is offered to clients for new product introductions? Would demonstration periods be included with this training?	6.67%	-	Yes, a combination of in-person, virtual trainings, and other supplemental trainings are offered.
-	4	Describe the on-site training available to UC employees upon delivery of new equipment. (Representative-conducted training sessions, videos, on-line training, manufacturer training, manuals, etc.)	6.67%	-	Trainings can range from the most basic use of equipment to thorough 2/4-day accredited training.
-	5	What are your firm's expectations of UC employees who will be responsible for operating and maintaining your brand's equipment?	-	-	Core Connect can be utilized by facility staff for registering of equipment, service requests, etc.
-	6	Are there any technological or structural requirements of the buildings your equipment will be placed in? Such requirements could be reinforced foundations, high impact flooring, high-speed internet access (please state hardwire or wifi requirements), or others the UC should be aware of. Responses do not have to be model specific (i.e. "All equipment requires WiFi access").	-	-	The attached Core Media Solutions has a full breakout that helps identify technology solutions.
-	7	What is your company's process for coordinating the repair of equipment still under warranty?	6.67%	-	Complete service experience within 72 Hours, with complete visibility through CoreConnect.
-	8	What is your company's process forrepairs that occur after the expiration of a warranty?	6.67%	-	Certified technicians are dispatched to complete work within the same 72-hour timeframe.
-	9	What is the timeline for replacement equipment that fails under normal operating conditions? What factors contribute to these timelines?	6.67%	-	While the 72-hour goal (from service request to service completion) is always the goal, certain factors can work against that, including pre-existing technician appointments and parts shortages. Both of these factors remain rare, and we take preventive measures in an attempt to avoid them.
-	10	Does your firm offer an on site parts library for all equipment in your portfolio, thata self maintaining department could utilize? If yes,	6.67%	-	Yes, a good example of this is at California State University – Northridge student recreation center
-	11	It is required that your firm (either direct or via manufacturer) provide a minimum 5 year warranty on your equipment.What are the requirements around that warranty?	6.67%	-	Core's warranties range 2-5 years, but our UC pricing discount includes a standard 5-year warranty.
-	12	Is your firm willing to negotiate at a department level on warranty and servicing options?	6.67%	Yes; No	Yes
-	13	Does your company offer a trade-in or buy back program?	6.67%	Yes; No	Yes
-	13.1	If Yes ,What is your process for determining the trade-in value given to customers for the equipment that is selected?	N/A	-	Value is determined through our extended network of authorized service providers and distributors.
-	14	What is your firm's process for the take-back and refurbishment or recycling of parts at the end of its useful life? Please state whether this is inclusive of your sustainability programs provided under the Sustainability Category or whether this is a separate process.	6.67%	-	Trade-in product is refurbished by either Core or one of our 3rd-party partners. Separate process.
-	15	Do you offer your entire product line for quick delivery? If not, which items are available for quick ship?	-	-	There are key goods in all product categories that are usually available for quick ship.
-	16	Does your company provide general quarterly business reviews? Please specify what type of information is included in your business reviews.	6.67%	-	Yes, several reports are available, covering financial, service, performance, etc.
-	17	Can your firm provide certification for UC employees on your equipment? Are the certificationsfocused on user training or maintenance training?	6.67%	-	Yes, both of these types of training are offered.
-	18	Have you had any warranty contract cancellations in the last 3 years? If so, why?	6.67%	-	No.
-	19	What type of product delivery logistics does your firm utilize?	6.67%	-	We offer a variety of delivery/pickup options to our network of distributors, customers, and freight

002295-Dec2020 - Fitness Equipment RFP - UC System-wide

Questionnaire Name: *	FOR MANUFACTURERS- Pricing
Questionnaire Type:	Commercial
Questionnaire Description:	Detailed pricing or simple discount off list for products and services

SECTION NAME	QUESTION NUMBER	QUESTION TITLE	QUESTION WEIGHT	RESPONSE OPTIONS	Fitness and Exercise Solutions LLC
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price **OR**acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	Model Name / Number	1.All Equipment **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price **OR**acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	Retail Price	1.Various **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price **OR**acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	UC Discount Price	1.Various **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price **OR**acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	Percentage Discount	1.45 **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	General Discount	
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	Equipment Discount	1.45
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	Parts Discount	
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	Service Discount	
-	3	Detail the various types of warranties and flexibility you've offered other clientswith their respective pricing models or if they are included with the purchase (i.e. full parts and service for 5 years, 3 year parts - 2year service, 5 year parts with no service). Warrantyprograms should offer a 5 year minimum term.	12.50%	-	We have offered a variety of warranty programs in the past, depending on market segment, customer preference, and a variety of other factors. We have a few products that come standard with 5-year parts and labor warranty, while the rest of our products follow the appropriate warranty term for the market segment. For the education channel, the designation is 3 years parts and 3 years labor unless an alternate program is worked out for the customer. We do offer the ability for our customers to certify their staff to perform service, both in and out of warranty. We can accommodate a 5-year warranty program term with appropriate costing built into offering (such as the case here with UC), or offered as an alternate add on option.
-	4	Please list the services your firm can offer in regards toownership of your equipment (cleaning, maintenance, training) and pricing listed along side the offering (mention if already included with purchase).	12.50%	-	There are many basic items offered at no additional charge, including access to Core Connect, as well as owner's manuals and corresponding maintenance plans. Cleaning specifications are also outlined in owner's manuals for each piece of equipment. We also offer added service items, including online support, predictive services and service contracts. We do extend full preventative maintenance programs, as well. Additional maintenance/service training offered at site specific level, traveling to regional service certifications, and/or our new online service certification opportunities. Costs vary depending on the scenario and what training is being covered.
-	5	If your firm is able to provide a "Balance of Line or Total Catalog" offering, what other value add services does your firm offer outside of cardio and strength training equipment? Please provide a list of products, services and associated percentage discount if applicable.	12.50%	-	We do offer a variety of educational/certification programs and opportunities: BOXMASTER EDUCATION 8 HOUR W/MASTER INSTRUCTORS$ 3,600 HUMAN SPORT AND STRENGTH TRAINING SPECIALIST EDUCATION 8 HOUR WITH MASTER INSTRUCTORS$ 3,600 SCHWINN EDUCATION 9 HOUR CLASSIC CERTIFICATION W/ MASTER INSTRUCTORS$ 3,200 SCHWINN EDUCATION 9 HOUR POWER CERTIFICATION W/ MASTER INSTRUCTORS$ 3,600 HIIT BY STAIRMASTER EDUCATION 4 HOUR W/ MASTER INSTRUCTORS$ 2,195 We can extend a 10% discount off any of the above for this group. At times, we may be able to reduce costs for programs outlined above, and even include, with large equipment purchases. There are also opportunities to sell seats for these training opportunities and help mitigate costs.
-	6	Does your firm provide a tiered discount structure to incentivize sales growth? If so, please describe below how that tiered structure would look and if it is based off UC System-wide spend or client specific.	12.50%	-	We do offer additional one-time purchase benefits, starting at $100,000, as well as annual sales volumes exceeding $1,000,000. Most commonly, future Product credits are applied to customer(s) in these scenarios, ranging from .25-3%, but this can vary, depending on the products and overall net profit margin for involved sales. These would be determined on case-by-case basis and as a part of monthly, quarterly, and annual business reviews.
-	7	Please list any additional discounts, rebates or credits you can offer. Examples could bebusiness volume, managing the business process, large orders, single location, growth, annual spend, guaranteed quantity, etc.	12.50%	-	Core is always open for negotiation when it comes to added-value benefits, on a case-by-case basis.
-	8	Are there any programs your firm offers that can increase discounts for UC purchases that havent been referenced previously in this RFP?	12.50%	-	Outside of case-by-case possibilities,fundraisers, sponsorships, and philanthropic initiatives.

002295-Dec2020 - Fitness Equipment RFP - UC System-wide

Questionnaire Name: *	FOR DEALERS - Pricing
Questionnaire Type:	Commercial
Questionnaire Description:	Detailed pricing or simple discount off list for products and services

SECTION NAME	QUESTION NUMBER	QUESTION TITLE	QUESTION WEIGHT	RESPONSE OPTIONS	Fitness and Exercise Solutions LLC
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price or acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	Model Name / Number	1.ALL **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price or acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	Retail Price	1.Various **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price or acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	UC Discount Price	1.Various **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	1	If submitting product specific pricing, please provide a listing of retail and discounted pricing offered for each piece of equipment under the scope of this RFP (Cardio and Strength Training Equipment). Your firm can choose to offer a contracted price or acontracted percent discount.**If preferred, please upload a document showing listed pricing for each piece of equipment.**	12.50%	Percentage Discount	1.45 **Attached Files :** Core Nautilus Strength Pricing.pdf;Core Schwinn Pricing.pdf;Core Stairmaster Pricing.pdf;Core Star Trac Cardio Pricing.pdf
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	General Discount	
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	Equipment Discount	1.45
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	Parts Discount	
-	2	If providing a percent (%) discount off retail, please state the discount in general or by specific category listed below.	12.50%	Service Discount	
-	3	Please provide a list of OEM equipment manufacturers that you partner with regularly. Please also provide a list and designate frequency of suppliers you have worked with in the past, but not regularly.	12.50%	-	Life Fitness (the entire family of products) and Dynamic Fitness. 10% frequency: Tuff Stuff.
-	4	Please list the services your firm can offer in regards toownership of your equipment (cleaning, maintenance, training) and pricing listed along side the offering (mention if already included with purchase).	12.50%	-	Although this would not apply to the University of California (due to geographical reasons), FES offers preventive maintenance contracts to many first-time and veteran fitness equipment owners. We currently have a contract customer list consisting of just over 200 customers
-	5	If your firm is able to provide a "Balance of Line or Total Catalog" offering, what other value add services does your firm offer outside of cardio and strength training equipment? Please provide a list of products, services and associated percentage discount if applicable.	12.50%	-	NA
-	6	Does your firm provide a tiered discount structure to incentivize sales growth? If so, please describe below how that tiered structure would look and if it is based off UC System-wide spend or client specific.	12.50%	-	NA
-	7	Please list any additional discounts, rebates or credits you can offer. Examples could bebusiness volume, managing the business process, large orders, single location, growth, annual spend, guaranteed quantity, etc.	12.50%	-	We typically offer the best price available from the inital quote.
-	8	Are there any programs your firm offers that can increase discounts for UC purchases that havent been referenced previously in this RFP?	12.50%	-	Certain orders can be discounted, based on specific surpluses or applicable vendor promotions.

Documents to Follow are from the For Dealers - Pricing Section - Question #1

Pricing Available Upon Request

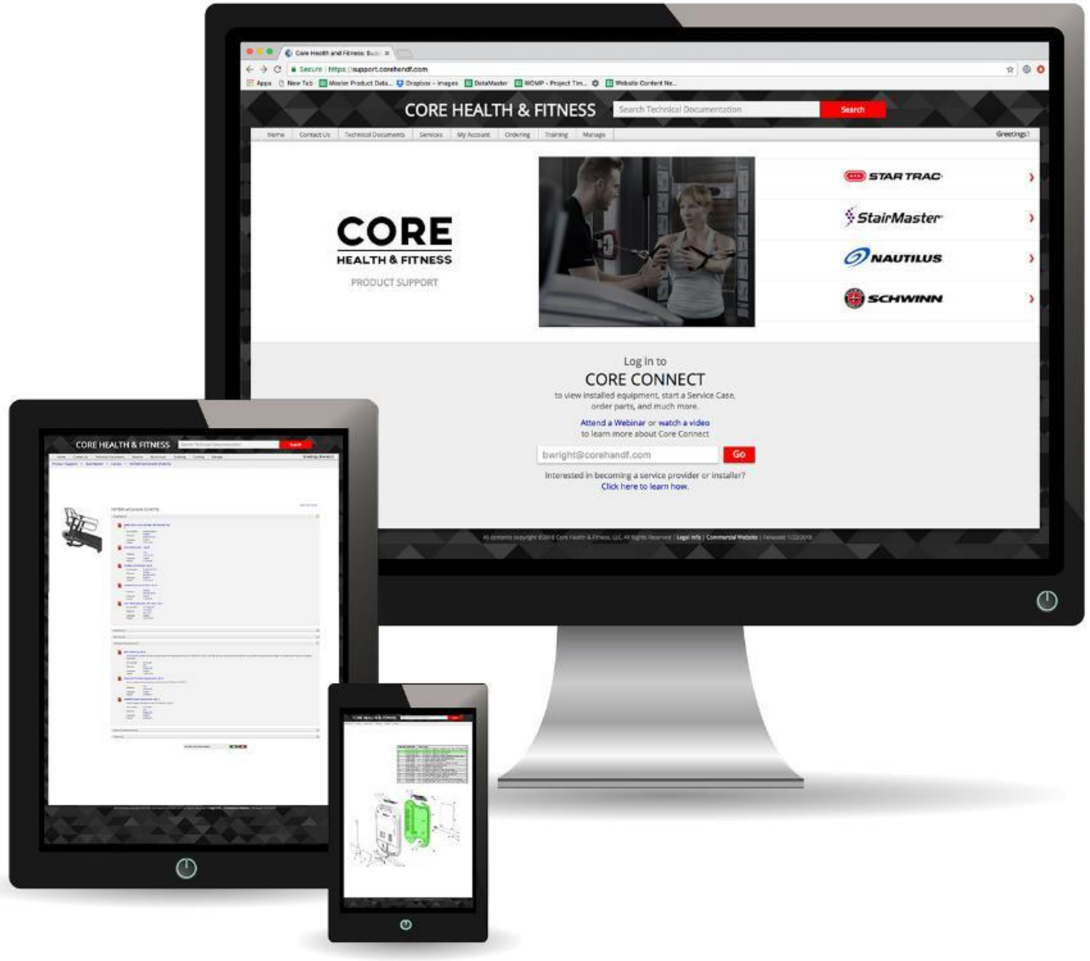
Additional Attachments

CORE CONNECT

Core Connect is your portal to all things service! Whether you need to order parts or register your warranty, Core Connect is the most effective way to get what you need fast and keep your facility operating smoothly.

CORE Connect Portal Features:

- General Inquiries
- Warranty Registration
- Preventative Maintenance
- Service Requests
- Parts Orders
- Automated partner payment
- Product technical library
- Transparency on service performance
- Real time communication



Log in to
CORE CONNECT
to view installed equipment, start a Service Case, order parts, and much more.

Attend a Webinar or watch a video to learn more about Core Connect

bwright@corehandf.com

Interested in becoming a service provider or installer? Click here to learn how.

To request access visit: Support.CoreHandF.com

Demand Planning

1. Demand Plan is generated based on historical sales and sales input for opportunity

a. That demand plan is rolled up on a global level by sales channel and sent to supply planning

2. Supply planners look at our current supply picture:

a. Inventory on hand

b. Inventory inbound (on the water)

c. Open purchase orders and timing of arrival

d. Open sales orders and customer request dates

3. That will develop what we call our supply plan.

a. Our supply plan is fed into our tactical planning models

b. Vendor forecasts are developed and sent out as necessary

4. Our tactical planning models are (1) Planning Tool excel model for Finished Goods (2) bolt on software for Oracle planning of Spares

a. Planning Tool

i. Allows us to see the baseline supply picture

ii. Looks at sales trends and forecast to optimize supply planning

iii. Planners adjust baseline plan based on supply constraints and sales trends while trying to maintain stock consistent with Safety Stock levels and open forecast

b. Oracle planning

i. Spares are looked at as a function of trend data

ii. We are massaging the trend data based on outlier bulk orders or sporadic demand

iii. Inventory movement between DC�s is crucial here.

1. We have some smaller vendors that can only ship to certain locations and we have to handle distribution.

2. The trends in different regions change and what was once moving fast in one location, may not move for a while and shift its movement to a different location

5. Weekly adjustments

a. On a weekly basis we are touching all SKU�s that are actively planned to look for variations in the plan.

i. Some may be expediting or pushing out

ii. Others may be shifting shipping location

6. We manage that all the way until it ships from the vendor.

CORE
HEALTH & FITNESS

StairMaster
SCHWINN
NAUTILUS
STAR TRAC

Core TV Media Solutions

Core Health & Fitness Set Top Box Solutions

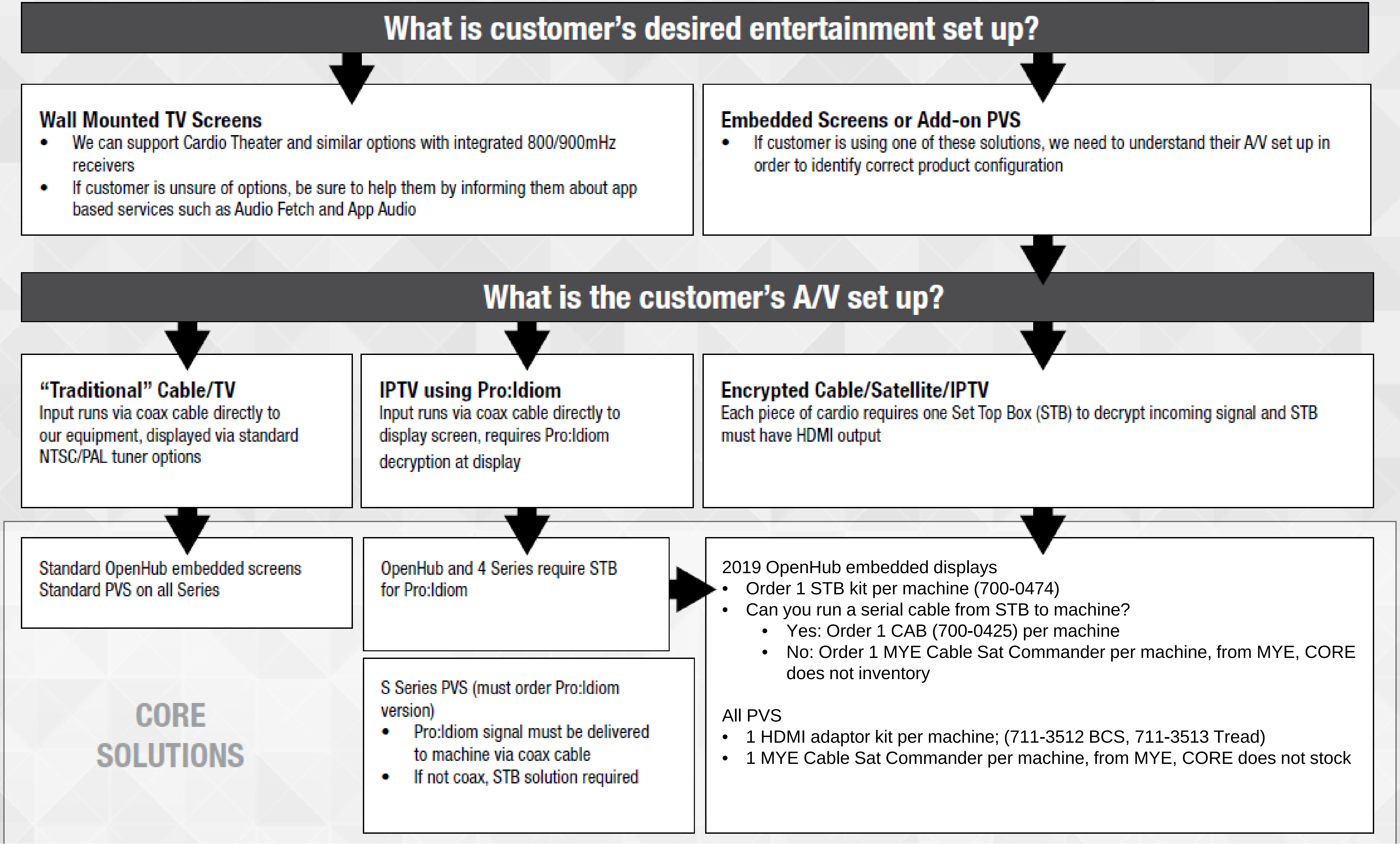
Customer solutions we provide:

- Embedded screen to display IPTV/Cable/Satellite content from Set Top Box (8/10-Series)
- PVS screens to display IPTV/Cable/Satellite content from Set Top Box (4/S/8/10-Series)
- PVS screen with built in Pro:Idiom capability for IPTV content (S-Series only)
- NOTE: we still provide standard embedded and PVS screens that will work with traditional unencrypted media solutions

Benefits of our solutions:

- Work with virtually any Set-Top-Box (STB) in the world
- Solutions for both embedded and PVS
- User control is done seamlessly from integrated display controls

Core Health & Fitness A/V Solutions



What is customer's desired entertainment set up?

Wall Mounted TV Screens

- We can support Cardio Theater and similar options with integrated 800/900mHz receivers
- If customer is unsure of options, be sure to help them by informing them about app based services such as Audio Fetch and App Audio

Embedded Screens or Add-on PVS

- If customer is using one of these solutions, we need to understand their A/V set up in order to identify correct product configuration

What is the customer's A/V set up?

"Traditional" Cable/TV
Input runs via coax cable directly to our equipment, displayed via standard NTSC/PAL tuner options

IPTV using Pro:Idiom
Input runs via coax cable directly to display screen, requires Pro:Idiom decryption at display

Encrypted Cable/Satellite/IPTV
Each piece of cardio requires one Set Top Box (STB) to decrypt incoming signal and STB must have HDMI output

CORE SOLUTIONS

Standard OpenHub embedded screens
Standard PVS on all Series

OpenHub and 4 Series require STB for Pro:Idiom

S Series PVS (must order Pro:Idiom version)

- Pro:Idiom signal must be delivered to machine via coax cable
- If not coax, STB solution required

2019 OpenHub embedded displays

- Order 1 STB kit per machine (700-0474)
- Can you run a serial cable from STB to machine?
  - Yes: Order 1 CAB (700-0425) per machine
  - No: Order 1 MYE Cable Sat Commander per machine, from MYE, CORE does not inventory

All PVS

- 1 HDMI adaptor kit per machine; (711-3512 BCS, 711-3513 Tread)
- 1 MYE Cable Sat Commander per machine, from MYE, CORE does not stock

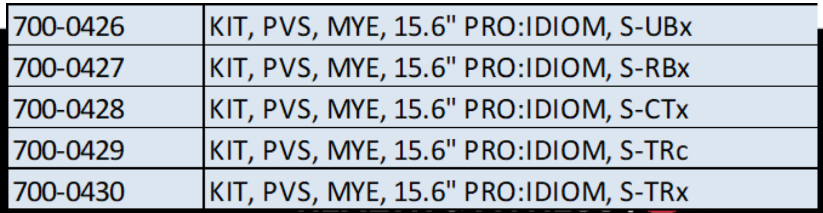
Three Questions to a Media Solution

Use these questions to determine the proper Core setup for entertainment

Note: if facility using wall mounted TVs, see information regarding 800/900mhz receivers at top of flow chart

1) What is your entertainment delivery system?

- “Traditional” cable system, unencrypted signal delivered to screen via coax cable:
  - Order standard PVS screens or embedded screens with on-board tuner appropriate for market - **DONE**
- IPTV/Satellite/Cable/any system that delivers encrypted signal to screens
- Special Case: Pro:Idiom entertainment system with Core S Series product
  - Requires one Pro:Idiom capable PVS screen per unit, these are different SKUs from standard S Series PVS:

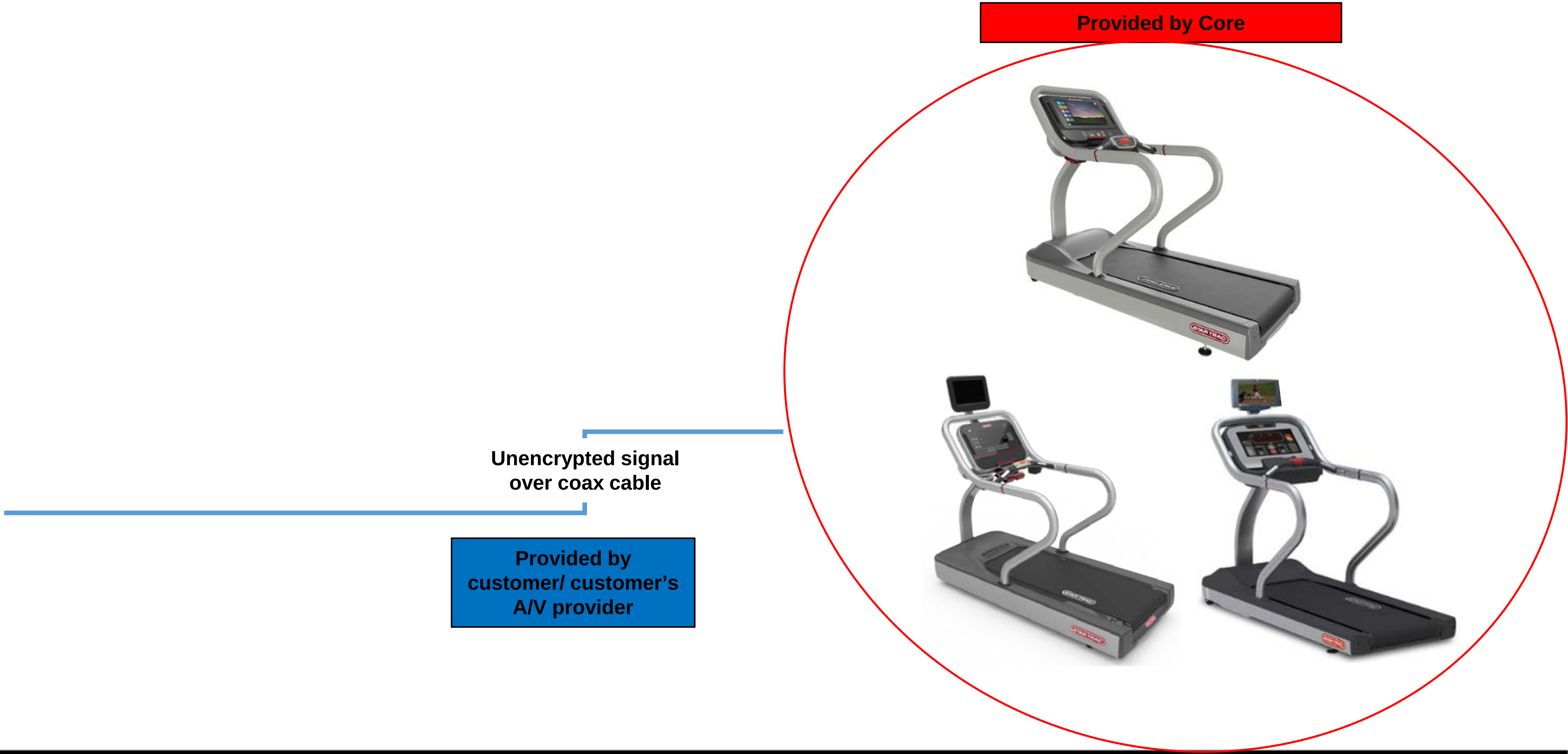


700-0426	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-UBx
700-0427	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-RBx
700-0428	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-CTx
700-0429	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-TRc
700-0430	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-TRx

Traditional Unencrypted Cable – 10/8/S-Series Embedded or PVS Solution

Customer Setup: Unencrypted signal delivered to base of cardio unit via Coax cable

Core Products: OpenHub embedded displays or PVS with correct TV tuner option



Provided by Core

Unencrypted signal over coax cable

Provided by customer/ customer's A/V provider

Pro:Idiom – S-Series PVS Solution (8/10 Series use STB solution)

Customer Setup: Pro:Idiom signal delivered to base of cardio unit via Coax cable

Core Products: S-Series w/PVS with Pro:Idiom tuner, SKUs below

Provided by Core

700-0426	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-UBx
700-0427	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-RBx
700-0428	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-CTx
700-0429	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-TRc
700-0430	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-TRx

Pro:Idiom encrypted signal over coax cable

Provided by customer/ customer's A/V provider

Core Health & Fitness Entertainment Delivery Solutions

Use these questions to determine the proper Core setup for entertainment
Note: if facility using wall mounted TVs, see information regarding 800/900mhz receivers at top of flow chart

1) What is your entertainment delivery system?

- “Traditional” cable system, unencrypted signal delivered to screen via coax cable:
- IPTV/Satellite/Cable/any system that delivers encrypted signal to screens
  - **2) PVS or Embedded screens?**
    - PVS:
    - Embedded Screens:
- Special Case: Pro:Idiom entertainment system with Core S Series product

Core Health & Fitness Entertainment Delivery Solutions

Use these questions to determine the proper Core setup for entertainment
Note: if facility using wall mounted TVs, see information regarding 800/900mhz receivers at top of flow chart

1) What is your entertainment delivery system?

- "Traditional" cable system, unencrypted signal delivered to screen via coax cable:
- IPTV/Satellite/Cable/any system that delivers encrypted signal to screens
  - **2) PVS or Embedded screens?**
    - PVS:
      - **3) Is STB located next to equipment or in remotely (A/V closet)?**
        - With equipment:
        - Remotely (A/V closet):
    - Embedded Screens:
      - **3) Is STB located next to equipment or in remotely (A/V closet)?**
        - With equipment:
        - Remotely (A/V closet):
- Special Case: Pro:Idiom entertainment system with Core S Series product

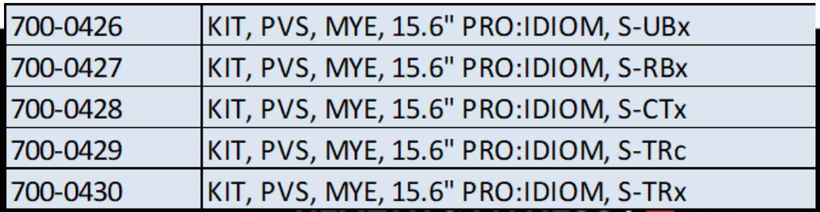
Core Health & Fitness Entertainment Delivery Solutions

Use these questions to determine the proper Core setup for entertainment

Note: if facility using wall mounted TVs, see information regarding 800/900mhz receivers at top of flow chart

1) What is your entertainment delivery system?

- "Traditional" cable system, unencrypted signal delivered to screen via coax cable:
  - Order standard PVS screens or embedded screens with on-board tuner appropriate for market - DONE
- IPTV/Satellite/Cable/any system that delivers encrypted signal to screens
  - 2) PVS or Embedded screens?
    - PVS:
      - 3) Is STB located next to equipment or in remotely (A/V closet)?
        - With equipment:
          - Requires one **STB per screen (provided by customer)**
          - Requires one **Broadcast Vision CAB per machine (700-0425)**
          - If STB output is HDMI, requires one HDMI kit, based on equipment type: 711-3512 BCS, 711-3513 Tread
        - Remotely (A/V closet):
          - Requires one **STB per screen (provided by customer)**
          - Requires one **MYE Wireless SatCommander** per machine, SKU: MWCS-AT9-STA, cost: $130 **(provided by MYE)**
          - If STB output is HDMI, requires one HDMI kit, based on equipment type: 711-3512 BCS, 711-3513 Tread
    - Embedded Screens:
      - 3) Is STB located next to equipment or in remotely (A/V closet)?
        - With equipment:
          - Requires one **STB per machine (provided by customer)**
          - Requires one **Core STB kit per machine (700-0474)**
          - Requires one **Broadcast Vision CAB per machine (700-0425)**
        - Remotely (A/V closet):
          - Requires one **STB per machine (provided by customer)**
          - Requires one **Core STB kit per machine (700-0474)**
          - Requires one **MYE Wireless SatCommander** per machine, SKU: MWCS-AT9-STA, cost: $130 **(provided by MYE)**
- Special Case: Pro:Idiom entertainment system with Core S Series product
  - Requires one Pro:Idiom capable PVS screen per unit, these are different SKUs from standard S Series PVS:

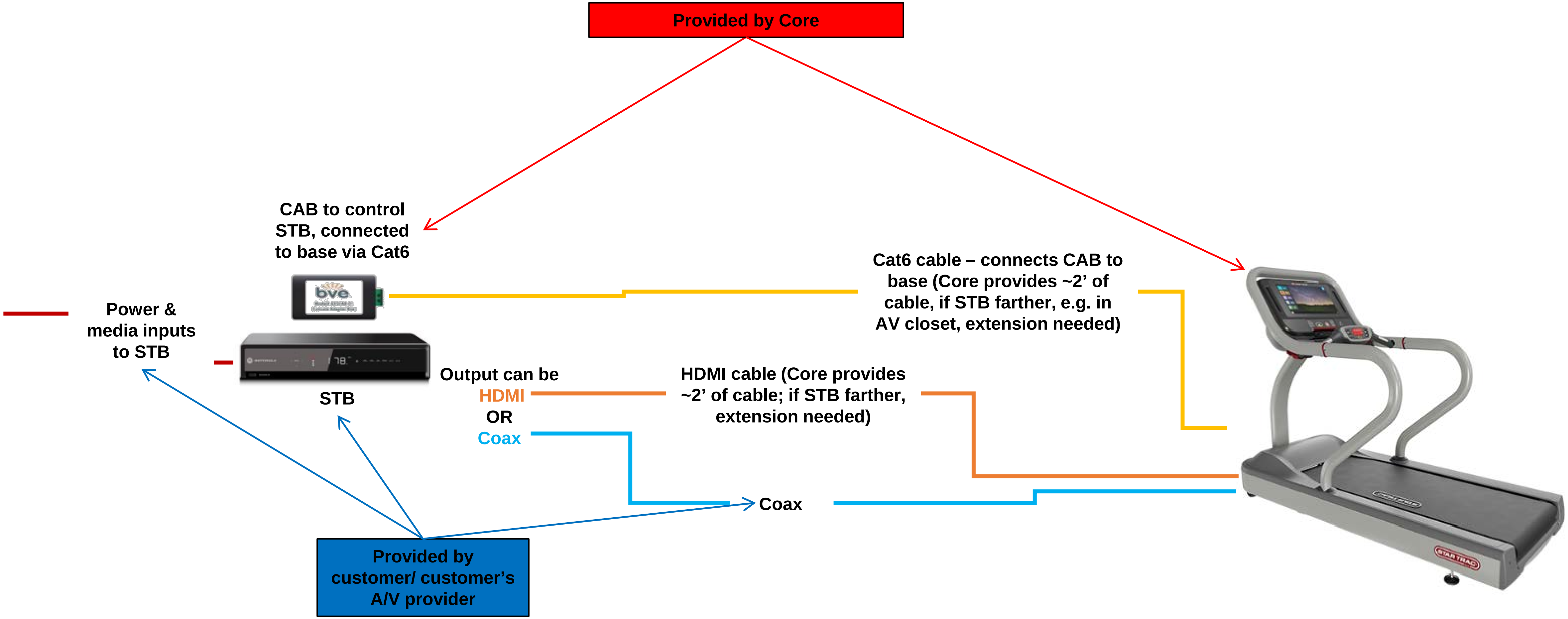


700-0426	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-UBx
700-0427	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-RBx
700-0428	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-CTx
700-0429	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-TRc
700-0430	KIT, PVS, MYE, 15.6" PRO:IDIOM, S-TRx

Encrypted Cable/Sat/IPTV – 10/8-Series 19”/15” Embedded Solution

Customer Setup: IPTV/Cable/Satellite installation using STB, **w/serial cable (Cat6)** from STB to equipment

Core Products: OpenHub embedded displays (8/10-Series) + 1 STB kit per machine (700-0474) + 1 CAB (700-0425) per machine



Provided by Core

CAB to control STB, connected to base via Cat6

Cat6 cable – connects CAB to base (Core provides ~2’ of cable, if STB farther, e.g. in AV closet, extension needed)

Power & media inputs to STB

STB

Output can be HDMI OR Coax

HDMI cable (Core provides ~2’ of cable; if STB farther, extension needed)

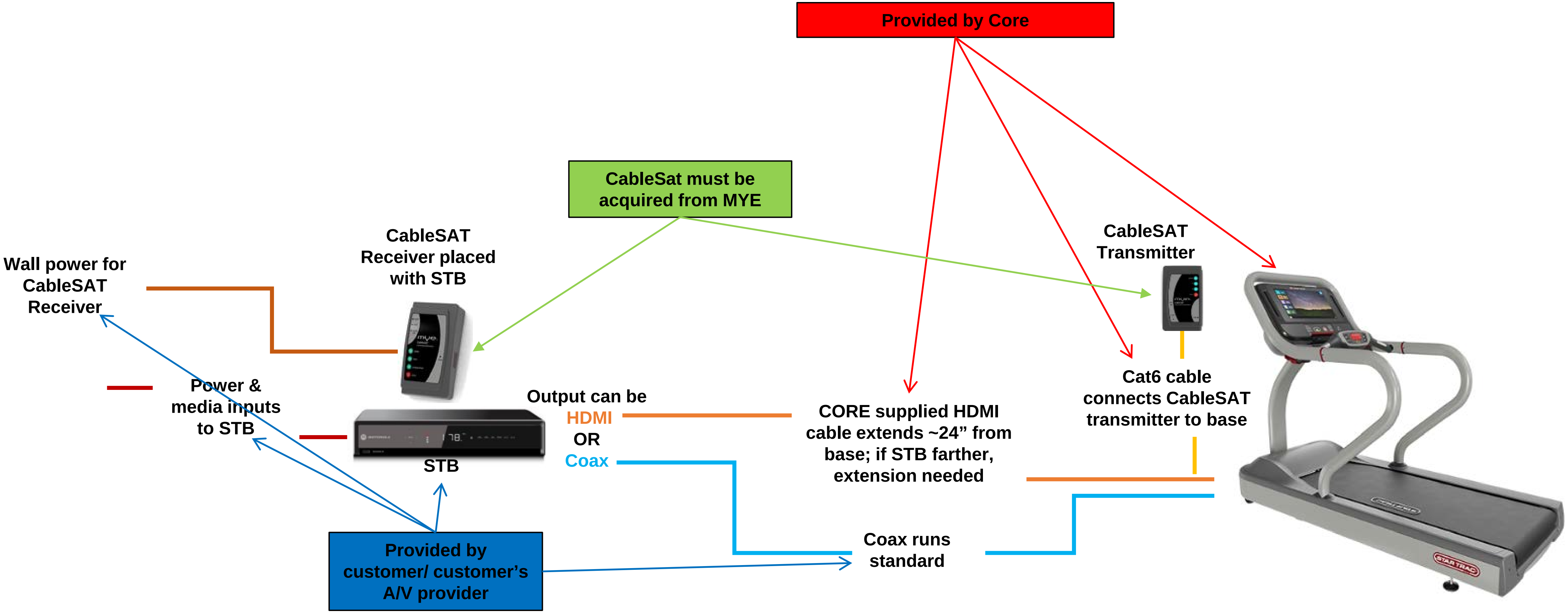
Coax

Provided by customer/ customer’s A/V provider

Encrypted Cable/Sat/IPTV – 10/8-Series 19”/15” Embedded Solution

Customer Setup: IPTV/Cable/Satellite installation using STB, no serial cable (Cat6) from STB to equipment

Core (&MYE) Products: OpenHub embedded (8/10-Series) + 1 STB kit/machine (700-0474) + 1 CableSat/machine from MYE



Provided by Core

CableSat must be acquired from MYE

Wall power for CableSAT Receiver

CableSAT Receiver placed with STB

Power & media inputs to STB

STB

Output can be HDMI OR Coax

CableSAT Transmitter

Cat6 cable connects CableSAT transmitter to base

CORE supplied HDMI cable extends ~24” from base; if STB farther, extension needed

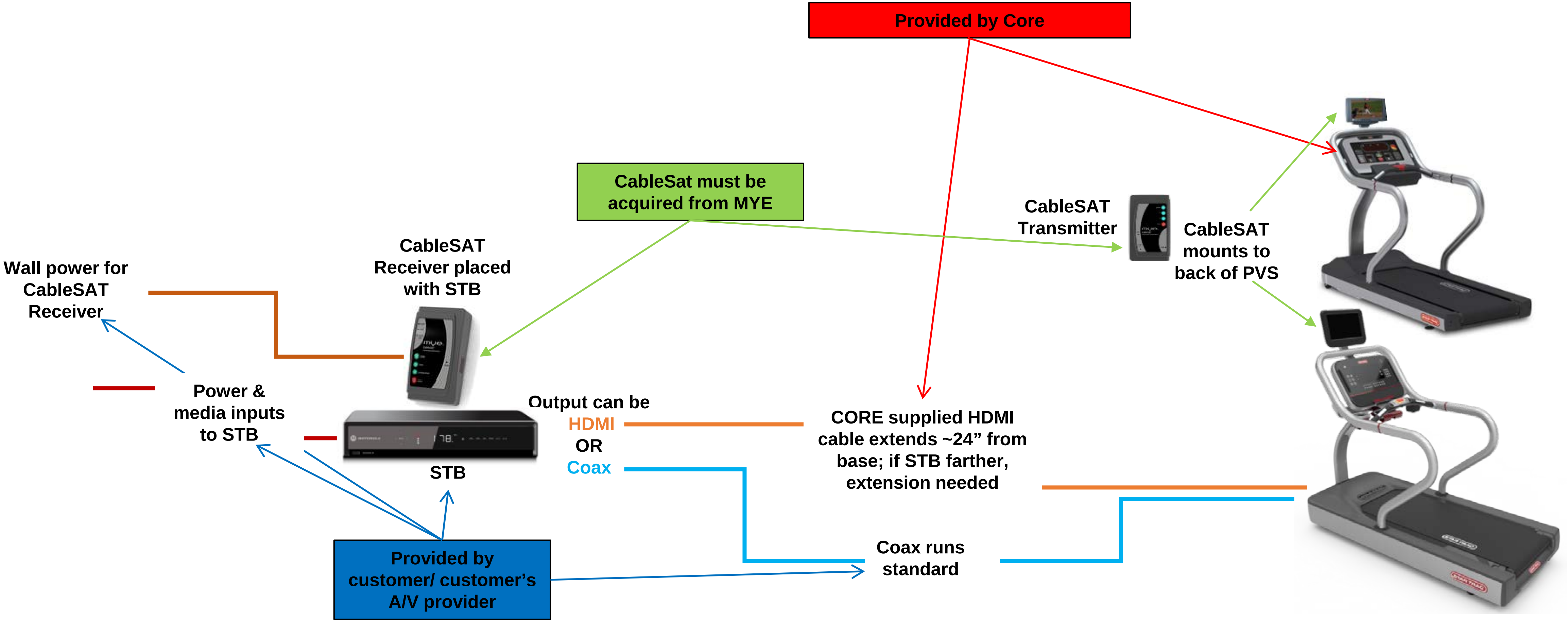
Coax runs standard

Provided by customer/ customer’s A/V provider

Encrypted Cable/Sat/IPTV – 10/8/S-Series PVS Solution

Customer Setup: IPTV/Cable/Satellite installation using STB

Core Products: 8/S-Series cardio products with PVS + 1 HDMI adaptor kit per machine; (711-3512 BCS, 711-3513 Tread)



Provided by Core

CableSat must be acquired from MYE

CableSAT Transmitter

CableSAT mounts to back of PVS

Wall power for CableSAT Receiver

CableSAT Receiver placed with STB

Power & media inputs to STB

STB

Output can be HDMI OR Coax

CORE supplied HDMI cable extends ~24" from base; if STB farther, extension needed

Coax runs standard

Provided by customer/ customer's A/V provider

CORE

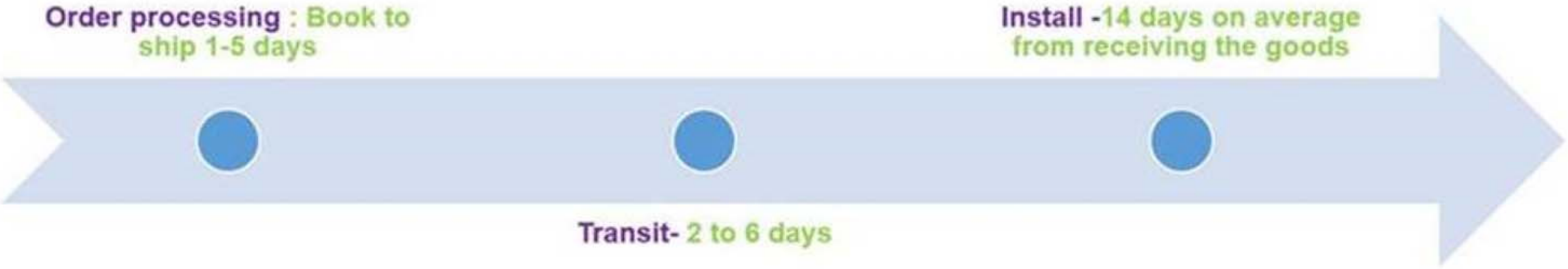
HEALTH & FITNESS

StairMaster®

SCHWINN®

NAUTILUS®

STAR TRAC®



Order processing : Book to ship 1-5 days

Transit- 2 to 6 days

Install -14 days on average from receiving the goods

UNIVERSITY
OF
CALIFORNIA

Sustainable Procurement Guidelines

Table of Contents

Glossary

The below definitions are copied directly from the UC Sustainable Practices Policy for reference, unless noted otherwise.

Addressable Spend: Spend that can be impacted through sourcing activities. For the purposes of this policy, addressable spend relates to the spend within a specific product or service category.

Catalog: A catalog is representative of a supplier's product information. A catalog is implemented in one of two formats: 1) through a hosted catalog or 2) through a punch-out catalog. See definitions for Hosted Catalog and Punch Out Catalog for more information. This definition is provided for clarification within the Guidelines and is not defined within the UC Sustainable Practices Policy.

Economically and Socially Responsible (EaSR) Spend: Spend on products or services supplied by a business holding one of the UC-recognized certifications listed the UC Sustainable Procurement Guidelines.

Environmentally preferable products: Designation for those products whose manufacture, use, and disposal results in relatively less environmental harm than comparable products.

Expanded Polystyrene (EPS): As defined by the City of San Francisco, blown polystyrene and expanded and extruded foams which are thermoplastic petrochemical materials utilizing a styrene monomer and processed by any number of techniques including but not limited to, fusion of polymer spheres (expanded bead polystyrene), injection molding, foam molding, and extrusion-blown molding (extruded foam polystyrene).

Full Time Equivalent (FTE): A full-time equivalent employee is the hours worked by one employee on a full-time basis and can be used to convert the hours worked by several part-time employees into the hours worked by full-time employees. A full-time employee is assumed to work 40 hours in a standard week.

Green Spend: Spend on products meeting the UC "Preferred Level" of environmental sustainability criteria as laid out in the UC Sustainable Procurement Guidelines.

Hosted Catalog: As defined in the JAGGAER technical manual, in simplest terms, a hosted catalog is an online version of a supplier's printed catalog. Hosted catalogs contain product data and details, along with pricing information for each item. When a product search is performed, the products in all of the hosted catalogs are searched. Hosted catalog search results contain product information from all suppliers depending on the search criteria entered by the user. This definition is provided for clarification within the Guidelines and is not defined within the UC Sustainable Practices Policy.

LEED^{TM}: Leadership in Energy and Environmental Design. LEED is a registered trademark of the U.S. Green Building Council (USGBC). This trademark applies to all occurrences of LEED in this document. LEED is a green building rating system developed and administered by the non-profit U.S. Green Building Council. The four levels of LEED certification, from lowest to highest, are Certified, Silver, Gold, and Platinum. LEED has several rating systems. This Policy refers to the following rating systems:

LEED for Interior Design and Construction (LEED-ID+C) for renovation projects;

LEED for Building Operations and Maintenance (LEED-O+M) for the ongoing operational and maintenance practices in buildings; and,

LEED for Building Design and Construction (LEED-BD+C) for new buildings and major renovations of existing buildings.

Location: As used in this Guidelines document, means any or all campuses. At this time, it does not include UC Health locations or the Lawrence Berkeley National Laboratory. This definition is provided for clarification within the Guidelines and defined differently within the UC Sustainable Practices Policy.

Packaging Foam: Any open or closed cell, solidified, polymeric foam used for cushioning or packaging, including but not limited to: Ethylene-vinyl acetate (EVA) foam, Low-density polyethylene (LDPE) foam, Polychloroprene foam (Neoprene), Polypropylene (PP) foam, Polystyrene (PS) foam (including expanded polystyrene (EPS), extruded polystyrene foam (XPS) and polystyrene paper (PSP)), Polyurethane (PU) foams, Polyethylene foams, Polyvinyl chloride (PVC) foam, and Microcellular foam. Not included is easily biodegradable, plant-based foams such as those derived from corn or mushrooms.

Policy Exception Authority: The responsible authority for granting exceptions to items III.G.5.a. and V.G.7. in the Sustainable Procurement sections of the UC Sustainable Practices Policy will be the Chief Procurement Officer for a non-UC Health systemwide or Office of the President contract and otherwise by the senior procurement officer of the campus.

Punch Out Catalog: Modified from the JAGGAER technical manual, punch-out catalogs are integrated external links to a supplier’s web-based catalog. The user exits the UC’s eprocurement site to search and select products from a supplier’s web catalog, then returns the items to the UC’s eprocurement shopping cart. The selected items are then submitted through the standard requisition/order process. This definition is provided for clarification within the Guidelines and is not defined within the UC Sustainable Practices Policy.

Required Level Green Spend criteria: The minimum certification standard required for a product or service category. Required Level Green Spend criteria is laid out in the UC Sustainable Procurement Guidelines.

Solicitation: The process of seeking information, bid proposals, and quotations from suppliers.

Sustainable Practices Policy: Refers to the University of California Sustainable Practices Policy, Governed by the UC Sustainability Steering Committee.

Sustainable Procurement: [Modified from the UK Government's Sustainable Procurement Task Force (2012)] Purchasing that takes into account the economic, environmental and socially responsible requirements of an entity's spending. Sustainable Procurement allows organizations to procure their goods and services in a way that achieves value for money on a whole-life basis in terms of generating benefits not only to the organization, but also to society and the economy, while remaining within the carrying capacity of the environment.

Sustainable Procurement Working Group (SPWG): Is the working group charged with improving the integration of sustainable principles and practices into the UC's procurement practices. The SPWG recommends changes to this document to the UC Procurement Leadership Council, and changes to the UC Sustainable Practices Policy to both the UC Procurement Leadership Council and UC Sustainability Steering Committee. See definitions for UC Procurement Leadership Council and UC Sustainability Steering Committee for more information. This definition is provided for clarification within the Guidelines and is not defined within the UC Sustainable Practices Policy.

Sustainable Spend: The intersection of Green and Economically and Socially Responsible (EaSR) Spend. UC Sustainable Spend is defined as spend that meets the criteria and requirements for Green Spend as well as EaSR Spend as laid out in the UC Sustainable Procurement Guidelines.

Total Cost of Ownership (TCO): An analysis of cost that considers not only purchase price, but also any costs associated with the acquisition, use, and disposal of the product. These costs may include some or all of the following: freight, taxes and fees, installation, operation/energy use, maintenance, warranty, collection, end-of-life disposal or recycling, as well as social or environmental costs, such as the cost of purchasing pollution offsets or monitoring labor practices.

UC Procurement Leadership Council (PLC): Is the system wide leadership council, composed of the Chief Procurement Officer (or equivalent) at each UC campus, charged with developing the overall strategic direction for the UC Procurement Services program that enables the organization to align objectives, initiatives, and projects to deliver on system wide procurement and supply chain initiatives. The PLC is ultimately responsible for the approval of changes and updates to this document. This definition is provided for clarification within the Guidelines and is not defined within the UC Sustainable Practices Policy. This definition is provided for clarification within the Guidelines and is not defined within the UC Sustainable Practices Policy.

UC Sustainability Steering Committee: Is the UC system wide committee charged with overseeing updates to and progress against the UC Sustainable Practices Policy. This definition is provided for clarification within the Guidelines and is not defined within the UC Sustainable Practices Policy.

1. Introduction and Document Purpose

The University of California's Sustainable Procurement Guidelines ("Guidelines") lay out the minimum sustainability requirements for products and services purchased by the University of California and identify those product attributes that are strongly preferred, if not mandatory.

The University of California's Sustainable Procurement Guidelines act as a companion to the Sustainable Procurement Policy and Procedure Sections of the UC Sustainable Practices Policy.

In general terms, the UC Sustainable Practices Policy outlines the University's targets for sustainable procurement as well as requirements for UC sustainable procurement practices, that is the activities of University of California buyers as they relate to sustainable procurement. This Guidelines document breaks down what the University considers to be sustainable at the product, product category, service or industry level.

The UC Sustainable Practices Policy prioritizes waste reduction in the following order: reduce, reuse, and then recycle. Accordingly, sustainable procurement should look to reduce unnecessary purchasing first, then prioritize purchase of surplus or multiple use products, before looking at recyclable, compostable, or otherwise sustainable products.

2. Document Guide

These Guidelines are intended to be used by the following parties, for the following purposes:

1. University of California, Office of the President, Strategic Sourcing Centers of Excellence and University Campus Procurement Services Departments (not including UC Health locations or the Lawrence Berkeley National Laboratory)
    a. To educate personnel purchasing on behalf of the University on Required and Preferred Green (environmentally) and Economically and Socially Responsible (EaSR) sustainability criteria to be included in solicitation specifications and reporting.
    b. To negotiate better pricing for products and services meeting the criteria described throughout these Guidelines and the Sustainable Practices Policy over traditional products and services, where opportunities exist.
    c. To develop language and specifications for solicitations stating that product and service offerings meeting the criteria described in these Guidelines will be required where they exist.
2. Department Level Buyers
    a. To educate personnel purchasing on behalf of the University on Required and Preferred environmental (Green) and Economically and Socially Responsible (EaSR) sustainability criteria when making purchasing decisions.

3. Reporting

Reporting will be required in line with the University of California sustainable purchasing targets and reporting requirements as outlined in the Sustainable Practices Policy (see III. Policy Text, G. Sustainable Procurement; V. Procedures, G. Sustainable Procurement). Reporting will be based on the percent spend in each of the following categories out of the total addressable spend. Reporting will commence by product or service category based on instruction in the sections below.

1. Green (environmentally preferable) Spend
2. Economically and Socially Responsible (EaSR) Spend
3. Sustainable Spend (the intersection of Green and EaSR Spend)

Clarification on each of these spend categories can be found in the sections below.

4. Green Spend

Green Spend is defined as spend on products meeting the UC Preferred Level of environmental sustainability criteria (see Table 1 below). The percentage of Green Spend is calculated using the following methodology, for a given product category over a particular period of time:

$$\frac{\text{Total spend on items meeting Preferred Level criteria in a given product category}}{\text{Total Addressable Spend in a given category}} \text{ x } 100$$

For example, the percent Green Spend calculation for computer electronics for Fiscal Year 16/17 is:

$$\frac{\text{Total Spend on EPEAT Gold registered computers during FY 16/17}}{\text{Total Addressable Spend on computers during FY 16/17}} \text{ x } 100$$

In addition to the above calculations, campuses may also calculate the “Dollar not Spent” to add to their overall Green Spend percentage. Please note that calculating the “Dollar not Spent” for an individual campus is optional and not required as part of a sites annual Green Spend reporting. Please see **Appendix I – The “Dollar not Spent” and Green Spend** to find more information on the various allowable methodologies to calculate the “Dollar not Spent.”

A. Green Spend General Criteria

Some Green (environmental) sustainability criteria are applicable across all, or a large number of different product or service categories. The following criteria must be applied to all applicable categories, and included in the specifications for all relevant solicitations and contracts.

1. ENERGY STAR® and WaterSense® certified products are required across all applicable product categories where price comparable (based on a total cost of ownership assessment) and consistent with the needs of University researchers, faculty, and staff.
2. Products and packaging shall be free of hazardous additives, including those mixed into the product and those used as surface treatments, unless no feasible alternative exists, and it is determined that the benefit outweighs the risk. Products and packaging must meet all eleven of the Kaiser Permanente Chemicals of Concern Criteria, including, but not limited to.
    a. Cadmium, mercury, lead, hexavalent chromium, polybrominated biphenyls, and polybrominated diphenyl ethers - All homogenous electronic parts are compliant with all European Union Restriction of the Use of Certain Hazardous Substances (EU RoHS) Directive's restricted limits (excluding exemptions).
    b. Polyvinyl chloride (PVC)
    c. Prop 65 Chemicals - Does not contain intentionally added chemicals listed by the State of California to cause cancer, birth defects, or reproductive harm that require warning or are prohibited from release to the environment under the California Safe Drinking Water and Toxic Enforcement Act of 1986 (Proposition 65). If contains Prop 65 chemicals, supplier must disclose Chemical Abstracts Service (CAS) #'s.
    d. Persistent, bioaccumulative and toxic chemicals (PBTs) - All homogeneous materials must contain less than 1000 ppm of PBTs.
    e. Organohalogen-based chemicals (bromine, chlorine, fluorine, and iodine)
    f. Antimicrobial/antibacterial agents[1] - Does not contain intentionally added antimicrobial/antibacterial agents to reduce surface pathogens.

B. Category Specific Criteria

Table 1 outlines the environmental sustainability criteria the University uses to define a given product category as "Green," for purposes of identifying products in hosted and punchout catalogs, and for calculating and reporting on Green and Sustainable Spend.

Recognized Certifications - These are reputable third party certifications the UC recognizes for identifying products that may have a reduced impact on humans and/or the environment. At a location's discretion, products with these certifications can be flagged as "light green" in hosted and punchout catalogs.

Required Level - These are the minimum mandatory requirements for each product category, which should be included in all relevant bid solicitations. Products and services that fall into these categories but do not meet these minimum requirements will not be listed in UC product catalogs except with the express request of campuses. Products in a given category must meet

[1] This includes hand and dish soaps labelled as antibacterial, except where required for use in hospitals and food service settings. Antimicrobials added to raw materials for the sole purpose of preserving the product are exempt, with the exception of triclosan and triclocarban which are explicitly prohibited.

all required level criteria listed, unless otherwise noted (e.g. if Energy Star and EPEAT Silver are listed, product must have both certifications).

Preferred Level - The Preferred Level of criteria is used for calculating Green and Sustainable Spend (see Section 6 below). At a location's discretion products meeting these criteria may be labelled as "dark green" in hosted and punchout catalogs, and shall be given preference during evaluation in all relevant bid opportunities, where price comparable (based on a total cost of ownership assessment) and consistent with the needs of University researchers, faculty, and staff. Products must meet all applicable Required Level criteria to qualify for Preferred Level criteria.

Table 1 - Category Specific Green Spend Criteria

Product or Service Category	Recognized Certifications and Standards	Required Level (minimum mandatory requirements)	Preferred Level
Electronics	ENERGY STAR ®	ENERGY STAR ®	ENERGY STAR ®
	EPEAT	EPEAT Bronze	EPEAT Gold
Cleaning Supplies	Green Seal	A minimum of 25% of purchases are certified by one of the recognized certifications	At least 75% of purchases are certified by of the recognized certifications
	UL Ecologo		
	EPA Safer Choice		
	FSC (for janitorial paper products)		
Office Supplies			
Copy Paper	FSC Recycled	A minimum of 30% PCRC or agricultural residue content (or GS-07 certified)	100% PCRC or agricultural residue content, or FSC Recycled labelled, with additional preference for paper that is PCF
	Post-consumer recycled content (PCRC)		
	Processed Chlorine Free (PCF)[2]		
	Green Seal (GS-07)		

[2] http://www.calrecycle.ca.gov/paper/chlorinefree/default.htm

	Agricultural residue[3] content		
Paper Office Supplies (other than copy paper)	FSC - Chain of Custody	A minimum of 30% PCRC[4]	100% recycled content with minimum 50% PCRC; 90% PCRC wire components; water-based or plant-based adhesives; and additional preference for PCF, FSC, and/or SFI labelled products[5]
	Sustainable Forestry Initiative (SFI)		
	Post consumer recycled content (PCRC)		
	Total recycled content		
	Processed Chlorine Free (PCF)		
	Green Seal (GS-07)		
Non-paper Office Supplies	Post-consumer recycled content (PCRC)	Meets the minimum CPG recycled-content levels for Non-Paper Office Products, and a minimum 30% recycled content for all writing utensils (dry-erase markers, highlighters, markers, pens, and pencils) or other plastic-based accessories	Meets the recycled content specifications in the Preferred EPP Specifications as listed by the Northeast Recycling Council (NERC), and free of antimicrobial coatings
	Total recycled content		
	Non-antimicrobial		
	EPA Comprehensive Procurement Guidelines (CPG)		
	Northeast Recycling Council (NERC) Model EPP Specifications and Purchasing Guidelines for Office Supplies		
Toner	Remanufactured[6]	Meets one of the	Meets both of the

[3] Must come from sustainably grown and harvested, non-GMO sources that do not replace forest stands or food crops

[4] Aligns with CA Department of General Services (DGS) Purchasing Standard DGS-441200-A for Paper Product Office Supplies and Northeast Recycling Council (NERC) Model EPP Specifications and Purchasing Guidelines for Office Supplies

[5] Modelled from Northeast Recycling Council's Preferred EPP Specifications for Paper Office Supplies

[6] Shall meet the State of California's Specifications for Remanufactured Toner and Ink Cartridges: https://www.documents.dgs.ca.gov/pd/epp/goods/officesupplies/inktonercartridges/20140902_Ink_Toner_Engineering_Spec.pdf

	High yield	recognized standards	recognized standards
Indoor Furniture	GREENGUARD Gold	Must meet all of the following: ● GREENGUARD Gold or SCS Indoor Advantage Gold ● Free of the 6 classes of chemicals of concern as described in Section 7.E.	Must have at least one of the following additional certifications: ● BIFMA Level certified (preference for 2 or 3) ● C2C Certified (preference for Silver or Gold) ● HHI compliant with published product list on their website ● FSC Certified wood ● Textiles certified by one of the recognized certifications ● Complete HPD ● Complete Declare label
	SCS Indoor Advantage Gold		
	Cradle to Cradle (C2C)		
	BIFMA Level		
	Meets the Healthier Hospitals Initiative (HHI) Safer Chemicals Challenge and is listed on the Healthier Hospitals Healthy Interiors Goal website		
	FSC (for products containing wood)		
	Textile certifications: ● GOTS ● Standard 100 by Oeko-Tex ● STeP by Oeko-Tex ● Cradle to Cradle ● Facts		
	Health Product Declaration (HPD)		
	Declare Label		
Compostable Food Service Ware	Biodegradable Products Institute (BPI)	Certified Compostable by BPI or GS-35, or made 100% from uncoated, unlined, obviously plant-based material, and appears on the Cedar Grove Accepted Items List	Meets additional criteria as described in the Compostable Food Service Ware section below
	Green Seal GS-35		
	Cedar Grove Accepted Items List for Commercial Compostability		
Water Appliances/ Fixtures	WaterSense®	WaterSense® Certified	WaterSense® Certified

5. Economically and Socially Responsible Spend

Economically and Socially Responsible (“EaSR”) Spend is defined as spend on products or services supplied by a business holding at least one of the UC-recognized classifications or certifications listed below. Recognized Certifications and Standards, listed in Table 2 below, outline the certifications and criteria that the University uses to define “EaSR” spend. Table 2 also includes a category for Preferred Certifications, which are certifications offered by California government agencies and/or of CA-based businesses. Currently there is no goal set for spend with suppliers meeting Preferred Certification standards.

The percentage of EaSR Spend is calculated using the following methodology, for a particular time horizon:

$$\frac{\text{Spend on products or services from a business that holds a UC-recognized EaSR certification}}{\text{Total Addressable Spend}} \times 100$$

A. EaSR Spend Criteria

Expenditures on products supplied by businesses holding at least one of the UC-recognized certifications and standards outlined under Recognized Certifications and Standards, see Table 2 below, will be considered EaSR Spend for the purposes of calculating the percent EaSR and Sustainable Spend.

> **Recognized Certifications and Standards** - These are reputable government or nationally recognized certifications and criteria the UC recognizes for identifying suppliers that may have a positive impact on society and/or the economy. Suppliers with these certifications should be flagged as a color or symbol differentiated like ‘green spend’ such as yellow in hosted and punchout catalogs.
>
> **Preferred Certifications** - These are reputable government or nationally recognized certifications and criteria the UC recognizes for identifying suppliers that may have a positive impact on society and/or the economy within California specifically. Suppliers with these certifications should be flagged as a color or symbol differentiated like ‘green spend’ such as yellow in hosted and punchout catalogs.

Table 2 - EaSR Spend Criteria

Business Classification	Recognized Certifications and Standards	Preferred Certifications
Small Business Enterprise	All government agency certifications and accepted third party certifiers such as: ● SBA-approved Third Party Certifiers Note that self-certification in SAM is	CA DGS certification or California state or local agency certification HUBZone certified

	accepted as well as any other small business certifications that also certify a businesses status as socially and economically disadvantaged such as (WOSB, SDVOSB, DBE, etc.)	SBA 8(a)
Disadvantaged Business Enterprise	All government agency certifications	All government agency certifications accepted, but principal office of business must be located in California and owners (officers, if a corporation) domiciled in CA.
Women-owned Business Enterprise	All government agency certifications	All government agency certifications accepted, but principal office of business must be located in California and owners (officers, if a corporation) domiciled in CA.
Minority Business Enterprise	All federal, state and local government agency certifications ● State and Local Government Certifying Agencies ● Federal includes (SBA 8(a), EPA, etc.)	All government agency certifications accepted, but principal office of business must be located in California and owners (officers, if a corporation) domiciled in CA.
Veteran-owned Business Enterprise	All government agency certifications	All government agency certifications accepted, but principal office of business must be located in California and owners (officers, if a corporation) domiciled in CA.
Service Disabled Veteran-owned Business Enterprise	All government agency certifications	DGS DVBE

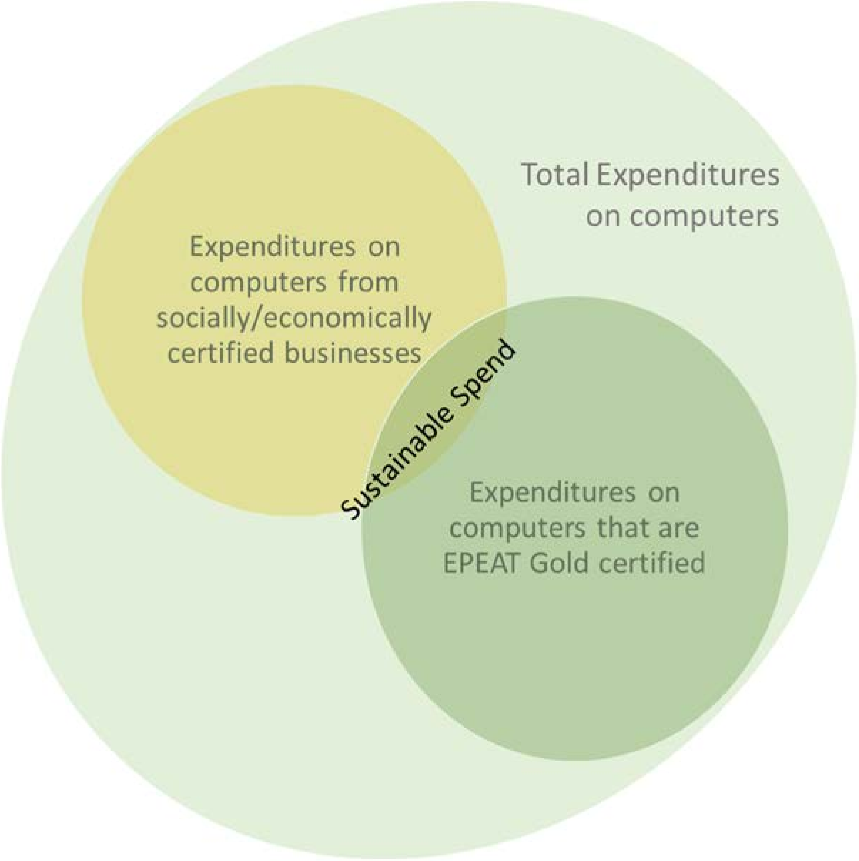
6. Sustainable Spend

Sustainable Spend is the intersection of Green and EaSR Spend. UC Sustainable Spend is defined as spend that meets the criteria and requirements in Section 4 for Green Spend and Section 5 for EaSR Spend (simultaneously). Thus, Sustainable Spend is defined as the expenditures on products in a particular product category that are supplied by a business holding one of the UC-recognized EaSR certifications, in addition to meeting the Preferred Level Green Spend criteria from Table 1.

An example of the percentage of Sustainable Spend calculated for computers (Figure 1) over a particular time horizon would be:

$$\frac{\text{Expenditures on EPEAT Gold certified computers from SBE businesses}}{\text{Total Addressable Spend on computers}} \times 100$$

Figure 1. Sustainable Spend for Computers


Total Expenditures on computers
Expenditures on computers from socially/economically certified businesses
Sustainable Spend
Expenditures on computers that are EPEAT Gold certified

7. Category Specific Specifications

These additional guidelines and specifications should be used during solicitations, contracting and as a reference when making department purchases. Minimum requirements for each product category are outlined in column three of table one. The below items are recommended for inclusion in RFPs. Other than those items referred to in Policy as mandatory, project teams need to determine which of the below items will be mandatory and preferred during the RFP development phase.

A. Electronics

Electronics includes any product for which an EPEAT certification is available. EPEAT currently includes product ratings for **PCs and Displays** (including tablets), **Imaging Equipment** (which includes printers, copiers, scanners and multifunction devices) and **Televisions**. Environmental leadership standards are currently under development with the intent to form the basis of future EPEAT categories for **Mobile Phones**, **Servers** and other electronic products (https://www.epeat.net/about-epeat/). Registration criteria and a list of all registered equipment are provided on the EPEAT registry.

In addition to the criteria established in Table 1, the University will ensure the following:

1. In accordance with Policy, all recyclers of the University's electronic equipment must be e-Steward certified by the Basel Action Network (BAN) (www.ban.org). In cases where the University has established take-back programs with a manufacturer, the University will require the manufacturer to become a BAN-certified e-Steward Enterprise (e-Stewards for Enterprises).
2. Printers and copiers must have duplex printing capabilities and hold their warranty while using 100% recycled content paper.
3. Suppliers shall be required to deliver items to the University with energy efficiency and duplex printing functions enabled.
    a. Departments will work with their IT departments to ensure that features remain enabled for the duration of the product's use.

B. Cleaning Supplies

Cleaning supplies include general purpose bathroom, glass and carpet cleaners; degreasing agents; biologically-active cleaning products (enzymatic and microbial products); floor-care products (e.g. floor finish and floor finish strippers); hand soaps and hand sanitizers; disinfectants; and metal polish and other specialty cleaning products. Also included are janitorial paper products such as toilet tissue, tissue paper, paper towels, hand towels, and napkins. Other janitorial products and materials (e.g. cleaning devices that use only ionized water or electrolyzed water) are excluded from this category.[7]

Disinfectants

All disinfectants must be EPA-registered, and contain only the following active ingredients: hydrogen peroxide, citric acid, lactic acid, thymol, or caprylic acid. As there is no sustainability certification for disinfectants, in order to increase your % Green Spend for Cleaning Supplies and follow green cleaning practices, it is recommended that each site assess its current usage and application of disinfectants. Disinfectant use should be limited to high-risk surfaces [locations where there is a higher risk for blood borne incidents, skin contact (MRSA risk), or contact with feces and body fluids] and where required by regulation. Microbes can be effectively removed from high-touch surfaces touched by multiple people throughout the day (door handles, faucet handles, handrails, drinking fountains etc.) by frequent and proper cleaning with a regular cleaning product.[8]

[7] Based on STARS Technical Manual Version 2.1, Administrative Update Three, July 2017

[8] UMass Lowell Toxics Use Reduction Institute's Guide to Safe and Effective Cleaning and Disinfecting: https://www.turi.org/Our_Work/Cleaning_Laboratory/Resources_and_Information/Disinfection/Guide_to_Safe_and_Effective_Cleaning_and_Disinfecting

C. Office Supplies

Copy paper - refers to standard office printing and copy paper.

Paper Office Supplies - includes Writing Paper (pads), Packing Paper, Folders, Letter folders, Expandable Filing Folders, Hanging folders or accessories, binders and indexes, Hanging Folders, Dividers, File Pockets, Standard Envelopes, Packaging Carton, Mailers, Easel Pads, Sticky Note, Storage Boxes, Desk Pad Calendar.

Non-paper Office Supplies - includes binders, clipboards, file folders, clip portfolios, presentation folders, plastic desktop accessories (desk organizers, desk sorters, desk and letter trays, and memo, note and pencil holders etc.), plastic envelopes, and writing utensils (dry-erase markers, highlighters, markers, pens, and pencils).

Toner - Additional recommendations can be found from the State of New York's Approved Specifications for Monochrome Toner Cartridges: https://www.ogs.ny.gov/greenny/specs/green-specs-MonochromeTonerCartridge.asp

E. Indoor Furniture

Furniture includes individual (e.g. task chair) and group seating; open-plan and private-office workstations; desks of all types, tables of all types; storage units, credenzas, bookshelves, filing cabinets and other case goods; integrated visual display products (e.g. markerboards and tackboards, excluding electronic display products); hospitality furniture; and miscellaneous items such as mobile carts, freestanding screens, and movable partitions. Movable partitions include office furniture system cubicle panels that are typically integrated with work surfaces, desks, and storage furniture. Furniture does not include office accessories, such as desktop blotters, trays, tape dispensers, waste baskets, all electrical items such as lighting and small appliances, and accessories such as aftermarket keyboard trays, monitor stands and monitor arms.

The University shall prefer furniture meeting specifications for the following hazardous chemical classes:

1. Flame Retardants: All furniture shall be free of flame retardant chemicals at levels above 1,000 parts per million in both standard and optional components, excluding electrical components.
    a. All upholstered seating subject to TB 117-2013 shall be labeled as not containing flame retardant chemicals consistent with the manner described in Section 19094 of the California Business and Professions Code.
    b. A product may contain flame retardants if required to meet code or regulation (e.g., TB 133 or ASTM E 1537), in accordance with the following criteria:
        i. No halogenated flame retardant chemical may be used at levels above 1,000 parts per million by weight of the homogeneous material, excluding electrical components.

    ii. Products that contain flame retardant chemicals that have been fully assessed using GreenScreen v1.2 (or newer) and meet the criteria for benchmark 2, 3, or 4 will be preferred.

2. Formaldehyde and Volatile Organic Compounds (VOCs): All furniture shall comply with ANSI/BIFMA e3-2014 Furniture Sustainability Standard, Sections 7.6.1 and 7.6.2, using either the concentration modeling approach or the emissions factor approach.
    a. Test results shall be modeled using the open plan, private office, or seating scenario in ANSI/BIFMA M7.1, as appropriate.
    b. Furniture products that additionally meet ANSI/BIFMA e3-2014 Section 7.6.3 and/or California Department of Public Health Standard Method v1.1 (emission testing method for California Section 01350) are preferred.
    c. Salvaged and refurbished furniture more than one-year old at the time of re-use is considered compliant, provided it meets the requirements for any site-applied paints, coatings, adhesives, and sealants.
    d. All composite wood materials, including hardwood plywood, particleboard, or medium density fiberboard, used in office, classroom, or healthcare furniture shall comply with Phase 2 of California's Code of Regulations, Title 17 §93120.2 – Airborne Toxic Control Measure to Reduce Formaldehyde Emissions from Composite Wood Products.
3. Per and Poly-Fluoroalkyl Substances (PFASs) used as stain/water/oil resistant treatments: All furniture shall be free of any long- and/or short-chain per- and poly-fluorinated alkyl compounds and fluorinated polymers used as stain, water, or oil resistant treatments above 100 ppm by weight of the homogenous material.
4. Antimicrobials: All furniture shall be free of any added or built-in chemical antimicrobials. Antimicrobials added to raw materials for the sole purpose of preserving the product are exempt, with the exception of triclosan and triclocarban which are explicitly prohibited.
5. Polyvinyl Chloride (PVC): All furniture shall be free of polyvinyl chloride (PVC) greater than 1% of product by weight, excluding electrical components. Electrical components that are free of PVC are preferred.
6. Heavy Metals: All furniture shall be free of any heavy metals, including hexavalent and trivalent chromium, in concentrations greater than 100 ppm.

F. Compostable Food Service Ware

Compostable food service containers and packages that have recycled and/or sustainably harvested content are preferred wherever possible.

1. All products must be certified compostable by the Biodegradable Products Institute (BPI) or Green Seal GS-35, proving that the finished product meets ASTM standards D6400 or D6868 for compostability. BPI-certified products can be accessed at: http://products.bpiworld.org/. Documentation may be required.

2. Products made 100% from paper, wood, bamboo or other obviously plant-based material, that are uncoated, unlined, or clay-coated (such as wooden stir sticks or uncoated paper plates) automatically meet this commercial compostability requirement without certification, so long as they appear on the Cedar Grove Accepted Items list for commercial compostability (https://cedar-grove.com/compostable/accepted-items), and the material type is disclosed.
3. Products with polyethylene liners are not compostable, and therefore do not meet the intent of these specifications.
4. Products shall not contain highly hazardous additives, including but not limited to persistent, bioaccumulative, or toxic chemicals (PBTs); carcinogens; mutagens; reproductive toxins, organohalogen-based chemicals (bromine, chlorine, fluorine or iodine); and endocrine disruptors.
5. Products shall not contain polyvinyl chloride (PVC), acrylonitrile butadiene styrene (ABS), polycarbonate (PC), polyurethane (PU), or any fluorinated chemicals. If product is fiber-based (including paper), ask for identification of the type of grease barrier or coating used.
6. Product is manufactured entirely with chlorine-free processing, meaning that no chlorine or chlorine compounds were used during manufacturing. Products may be unbleached or whitened in a chlorine-free process (if certified process chlorine-free).
7. Paper products are made from 40% post-consumer recycled content or 100% total recycled content (pre- or post- consumer), unless intended for hot beverages, in which case they are made from a minimum of 10% post-consumer recycled content. Bidder should disclose the amount and type of recycled content.
8. Non-cutlery products contain at least 90% biobased carbon content; cutlery products contain at least 70% biobased carbon content. Bidder can provide documentation demonstrating that its biobased carbon content meets the above specifications through one of the following:
    a. ASTM Standard D6866 laboratory test data
    b. USDA's BioPreferred Label
    c. Products made of 100% uncoated wood, bamboo, paper or other obviously fiber-based material will automatically meet these biobased content requirements. Samples may be requested.
9. Product shall not contain added engineered nanomaterials.
10. Product materials were sustainably produced and are certified as one of the following:
    a. Forest Stewardship Council (FSC)
    b. Protected Harvest
    c. Rainforest Alliance
    d. Fair Trade USA
11. Feedstock and final product are produced in North America.
12. Product material grown without genetically modified organisms and certified to be GMO-free by one of the following:
    a. Non-GMO Project Verified (www.nongmoproject.org)
    b. CERT ID NonGMO
    c. ProTerra Certifications (www.geneticid.com/services/certification)

13. Product is made from sustainably grown, non-food agricultural resources such as perennial biomass crops and sustainably harvested residues (for more information, see the Sustainable Bioplastic Guidelines: https://healthybuilding.net/uploads/files/sustainable-bioplastic-guidelines.pdf
14. Product is EcoLogo or Green Seal-certified by one of the following:
    a. EcoLogo CCD-084 (Table Napkins),
    b. EcoLogo CCD-085 (Kitchen Towels),
    c. EcoLogo CCD-086 (Hand Towels),
    d. Green Seal GS-1 (Sanitary Paper Products),
    e. Green Seal GS-9 (Paper Towels and Napkins),
    f. Product meets the standard for biodegradability in the marine environment (ASTM D7081-05).
15. Inks for printing and graphics are vegetable-based and approved for use by U.S. Food and Drug Administration, where required.

G. Water Appliances/Fixtures

This category includes all products covered by WaterSense including residential toilets, showerheads, bathroom faucets, commercial toilets, urinals, pre-rinse spray valves, irrigation controllers, and spray sprinkler bodies.

8. Best Practices for Procurement Services[9]

1. Market basket lists can be used as a tool for increasing the purchase of sustainable products at competitive and affordable prices. By only including products meeting the Required and Preferred Level of sustainability criteria in a market basket list, the University may be able to achieve reduced rates that will in turn direct spend towards sustainable products over conventional products. Allowing for revisions to the market basket beyond traditional changes in volume/spend patterns may allow for more competitive pricing on newly added sustainable items.
2. Through solicitation specifications and contract provisions, suppliers are required to:
    a. Clearly identify UC-recognized “light green” and “dark green” sustainable items in product catalogs.
    b. Ensure that any additional sustainability symbols/icons/certifications are displayed along with attribute details per product (e.g. a product with a recycled content symbol must also have in its product description details about the % total recycled content and % post consumer recycled content).
    c. Offer capabilities to:

[9] Modified from: https://nerc.org/documents/EPP/Office%20Supplies/EPP%20Specs%20-%20Office%20Supplies.pdf

    i. Block and/or restrict pre-identified conventional items from being purchased online so University employees are compelled to purchase products that are in compliance with UC's Sustainable Procurement Policies and Guidelines.
    ii. Auto-substitute pre-identified conventional products with sustainable products on the market basket list when end-user places conventional item in online cart.

  d. Make sustainable items display first in online catalog search results, or make them easily found within online product catalogs through effective search tools, search filters, and related navigational tools.
  e. Incentivize consolidated deliveries whenever feasible (e.g. deliveries only on certain days of the week or reduced pricing for consolidated shipping).
    i. Document or illustrate how the delivery consolidation method reduces the UC and supplier's carbon footprint (e.g. reduction in fossil fuel use, carbon emissions, packaging materials, or on-site vehicle traffic).
  f. Use only delivery service companies that are participants in EPA's Smartway Program.

3. LEED credits should be incorporated into all materials procurement associated with new facility constructions and major renovations.[10]

9. Certification and Standards Definitions

a. BIFMA Level® - BIFMA Level is a multi-attribute furniture certification based on the ANSI/BIFMA e3 standard, addressing material use, energy, atmosphere, human and ecosystem health, and social responsibility at the product, facility, and organizational level. Certification is based on a points system with three levels of achievement, from Level 1 through Level 3.
b. Biodegradable Products Institute (BPI) - BPI is a non-profit organization with the largest certification program for compostable products and packaging in North America. Their single-attribute certification indicates compliance with the ASTM D6400 and/or D6868 standards for commercial compostability.
c. Cradle to Cradle TM - Cradle to Cradle is a multi-attribute standard that evaluates a wide range of products across five categories of human and environmental health, including Material Health, Material Reutilization, Renewable Energy and Carbon Management, Water Stewardship, and Social Fairness. Product certification is awarded at five levels, from Basic to Platinum, with an emphasis on continuous improvement.
d. ENERGY STAR ® - Energy Star is a standard for energy efficient consumer products administered by the U.S. Environmental Protection Agency and the U.S. Department of Energy.
e. EPA Safer Choice - Formerly known as Design for the Environment (DfE), the Safer Choice label is the U.S. Environmental Protection Agency's program to identify products with safer chemical ingredients.[11]
f. EPEAT ® - The Electronic Product Environmental Assessment Tool is a method for consumers to evaluate the effect of a product on the environment. It ranks products as gold, silver or bronze

[10] https://www.phoenix.gov/oepsite/Documents/070520.pdf

[11] Definition taken from STARS Technical Manual Version 2.1, Administrative Update Three, July 2017

based on a set of environmental performance criteria. It is managed by the Green Electronics Council.

g. FACTS - Facts is a sustainability certification program for commercial textiles, recognizing textiles conforming to the NSF/ANSI 336 multi-attribute standard, evaluating a textile for environmental, economic and social aspects across its life cycle. Facts utilizes four conformance levels from Compliant to Platinum.

h. Forest Stewardship Certification - The Forest Stewardship Council (FSC) is an independent, non-profit organization that protects forests for future generations. FSC Chain-of-Custody certification traces the path of products from forests through the supply chain, verifying that FSC-certified material is identified or kept separated from non-certified material throughout the chain. FSC Forest Management certification confirms that a specific area of forest is being managed in line with the FSC Principles and Criteria.[12]

    i. FSC Recycled - The FSC Recycled on-product label means all the wood or paper in the product comes from reclaimed (re-used) material.[13]

i. Global Organic Textile Standard (GOTS) - GOTS is a textile processing standard for organic fibres, which includes both ecological and social criteria, from harvesting of raw materials through manufacturing and labelling.

j. GREENGUARD ® - The GREENGUARD Environmental Institute certifies products and materials for low chemical emissions. Greenguard Gold ensures that a product is safe for use in schools and healthcare facilities, and is referenced by LEED.

k. Green Seal ® - Green Seal is an independent nonprofit organization "dedicated to safeguarding the environment and transforming the marketplace by promoting the manufacture, purchase, and use of environmentally responsible products and services." The Green Seal certification is based on multi-attribute environmental standards that meet the ISO 14024 standards for eco-labeling.[14]

l. Healthier Hospitals Healthy Interiors Goal (HHI) - The Healthy Interiors Goal aims to promote public and environmental health, and urge the furnishings market to develop safer products, while reducing disposal costs and liability. Furniture and textiles that meet the Healthy Interiors Goal claim contain no formaldehyde, perfluorinated compounds, polyvinyl chloride, antimicrobials, or flame retardants above the specified minimum levels. Products meeting the Goal must be listed on the website, and are not verified.

m. Process Chlorine Free (PCF) - PCF means that no chlorine or chlorine derivatives were used in the recycling process. Paper that was originally bleached with chlorine or chlorine derivatives may be used as feedstock, however. Only paper that is "totally chlorine-free" (TCF) is produced with pulp that has been bleached without any type of chlorine or chlorine derivative, or has not been bleached.[15]

[12] Ibid

[13] https://ic.fsc.org/en/choosing-fsc/fsc-labels

[14] Definition taken from STARS Technical Manual Version 2.1, Administrative Update Three, July 2017

[15] http://www.calrecycle.ca.gov/paper/chlorinefree/default.htm

n. STANDARD 100 by OEKO-TEX® - Certification for raw, semi-finished, and finished textile products at all processing levels, as well as accessory materials used. Criteria focuses on product safety based on test criteria for numerous harmful chemicals.

o. STeP by OEKO-TEX® - STeP assesses against criteria for sustainable, environmentally and socially responsible textile and apparel production and logistic sites, addressing the reduction of hazards and risks throughout the production chain, with the goal of improving factory resource efficiency.

p. UL Ecologo - The UL Environment ECOLOGO program certifies products, services and packaging for reduced environmental impact. ECOLOGO Certifications are voluntary, multi-attribute, lifecycle based environmental certifications that meet the ISO 14024 standards for eco-labeling.[16]

q. WaterSense® - WaterSense is a U.S. Environmental Protection Agency program designed to encourage water efficiency in the United States through the use of a special label on consumer products.

10. Packaging Foam Ban Guidance

In accordance with section III.F.5. of the UC Sustainable Practices Policy, the University has prohibited the sale, procurement and/or distribution of packaging foam UC-wide. The following guidance is meant for sourcing and procurement professionals within UC and is intended to leverage large sourcing opportunities to mitigate single use packaging foam waste in support of UC's Zero Waste goals.

1. Scope

   The ban of expanded plastic foam materials in packaging is effective as of January 1st, 2020. The ban applies to all packaging brought onto UC campuses via the purchase of goods on behalf of the University. The only exception to this ban is for the purchase of products utilized in laboratory or medical settings.

2. Enforcement

   This ban is a requirement of the UC Sustainable Practices Policy in support of UC's Zero Waste goal. UC Terms and Conditions include the policy language regarding this ban, which must be addressed when contracting with suppliers for the purchase of goods. When conducting a competitive solicitation for goods, the University must incorporate language into all Requests For Proposals/Quotes/etc. (RFx's) articulating this ban, including in the qualitative assessment process, and ensure that it is addressed as part of the final award of business.

   If a supplier claims to be unable to meet the requirements of the ban, an exemption will need approval in accordance with the instructions provided below. The exemption process is not required for one-time purchases. In the case of one-time purchases, the supplier should be required to take back any non-compliant packaging upon delivery. For existing UC contracts (contracts executed prior to January 1, 2020), enforcement of this ban (including a possible

[16] Definition taken from STARS Technical Manual Version 2.1, Administrative Update Three, July 2017

exemption request) must be addressed during the next contract amendment, extension or as part of a new award.

3. Exemption Process
   If a supplier claims to be unable to meet UC's ban on expanded plastic foam material in packaging and UC still intends to do business with that supplier under a contract for goods, then the supplier must apply for an exemption to the ban. To do so, they must submit a completed foam packaging ban exemption form including all required documentation to substantiate claims in support of the exemption. Download the **Request for Exemption Form** from the UC Systemwide Forms & Documents page: https://www.ucop.edu/procurement-services/policies-forms/index.html.

   Suppliers are to submit their Foam Packaging Ban Exemption Form to the Commodity Manager, Buyer or other employee authorized to contract for goods on behalf of UC. The designated Policy Exception Authority (see Glossary) must grant approval of all exemption requests. A copy of all submitted (approved and declined) Foam Packaging Ban Exemption Forms must be submitted to the appropriate Sustainability Office for reference.

11. Approval procedure updates and changes

Changes to this document must be approved by the UC Procurement Leadership Council (PLC) on the recommendation of the Sustainable Procurement Working Group.

12. Change Log

Approval Date	Summary of Changes	Approved by	Product/Service Categories Impacted	Start Date for Reporting on New or Updated Categories
1/2/19	Added Packaging Foam and Policy Exception Authority definitions to Glossary; added new Section 10. Packaging Foam Ban Guidance	UC Procurement Leadership Council	All where product packaging is involved.	n/a
8/10/18	Implementation of UC Sustainable Procurement Guidelines	UC Procurement Leadership Council	Electronics, Cleaning Supplies, Copy Paper, Paper Office Supplies (other than copy paper), Non-paper Office Supplies, Toner, Indoor Furniture, Compostable	7/1/2018

			Food Service Ware, Water Appliances/Fixtures	

Appendix I - The “Dollar not Spent” and Green Spend

As with waste, the hierarchy of environmentally sustainable spend starts with reduce and reuse. As such, in the assessment of Green Spend, the “dollar not spent” can be included in Green spend calculations. This concept is addressed in the following section. Please note that calculating the “Dollar not Spent” for an individual campus is optional and not required as part of a sites annual Green Spend reporting (outlined in section 4. Green Spend above).

How to calculate the dollar not spent:
Items that are not purchased due to education and reduction activities and/or items that are reused on campus may be added to the Green Spend calculation at a location’s discretion. The process for adding these to the Green Spend calculation is as follows:

$$\frac{\text{Green Spend purchase per category + approximate market value of goods not purchased}}{\text{Addressable spend per category + approximate market value of goods not purchased}} \times 100$$

To determine the approximate value of goods not purchased, locations should use an appropriate combination of the below methodologies:

Method 1: Reuse (for example, goods reused from surplus operations)

STEP 1. Determine the current market value of the goods were they to be purchased new.

STEP 2. Sum the product cost (quantity of goods x current market value of goods).

STEP 3. Include the current market value of goods in the numerator and denominator of the Green Spend calculation.

Where:
<u>Current market value of goods</u> is to be determined as the average purchase price of the equivalent good available on system wide contracts (or an average market value of equivalents if no system wide contract exists).

Method 1 Example: 4 desks and 3 desk chairs re-used on campus in surplus operations.

STEP 1: Determine the average cost for the 4 desks and 3 desk chairs from relevant system wide contracts (e.g. average cost of desk is $2000 each, average cost of chair is $1,500 each).

STEP 2. Sum the product cost of the items (4 x $2,000) + (3 x $1,500) = $12,500

STEP 3. Include the market value of the goods in the numerator and denominator for the calculation for green spend;

$$\frac{\text{Green Spend purchase per category + \$12,500}}{\text{Addressable spend per category + \$12,500}} \times 100$$

Method 2: Normalized Reduction in Purchase of Commodity Goods

Where:

Product use (goods purchased) is a function of the number of staff/users.

STEP 1. Determine the quantity of goods purchased per driver in a baseline year:

Equation:	**For example:**
$\frac{\text{Baseline quantity of goods consumed}}{\text{Baseline quantity of driver}}$	$\frac{\text{Baseline \# reams of copy paper purchased}}{\text{Baseline \# Full Time Equivalent staff}}$
	$\frac{\text{Baseline \# gallons of cleaning products purchased}}{\text{Baseline \# square feet of cleaned space}}$

STEP 2. Determine the quantity of goods purchased per driver in the current year using equations as above:

Equation:	**For example:**
$\frac{\text{Current quantity of goods purchased}}{\text{Current quantity of driver}}$	$\frac{\text{Current \# reams of copy paper purchased}}{\text{Current \# Full Time Equivalent staff}}$
	$\frac{\text{Current \# gallons of cleaning products purchased}}{\text{Current \# square feet of cleaned space}}$

STEP 3. Determine the total difference in the quantities of goods purchased between the baseline and current years (savings) using the following equation:

Equation:

Current quantity of driver x (Baseline quantity of goods per driver - Current quantity of goods per driver)

Example:

<u>Paper</u>: Current number of FTEs x (Baseline number of reams of copy paper purchased per FTE - Current number of reams of copy paper purchased per FTE)

<u>Cleaning</u>: Current number of sq. ft. cleaned x (Baseline number of gallons of cleaning product purchased per sq. ft. cleaned - Current number of gallons of cleaning product purchased per sq. ft. cleaned)

STEP 4. Determine the value of savings based on the current market value of goods.

STEP 5. Include the current market value of goods in the numerator and denominator of the Green Spend calculation.

Where:

Current market value of goods: is to be determined as the average price of the equivalent good available on system wide contracts (or an average market value of equivalents if no system wide contracts product available).

Note that if the purchase of one commodity is replaced with purchase of a different (but similar) commodity, this should not be considered a reduction.

Method 2 Example (Using copy paper as example good):

STEP 1: Determine the quantity of goods purchased per driver in baseline year
Baseline year: 2005/06 FY
Quantity of goods purchased: 500 reams of copy paper/year
Driver: 800 Full Time Equivalent staff
Number of reams of copy paper purchased per FTE: 500/800 = .625 reams per FTE

STEP 2: Determine the quantity of goods purchased per driver in current year
Current year: 2017/18 FY
Quantity of goods purchased: 500 reams of copy paper/year
Driver: 1500 Full Time Equivalent staff
Number of reams of copy paper purchased per FTE: 500/1500 = .33 reams per FTE

STEP 3: Determine savings per driver between baseline and current year
Current # FTEs x (reduction in reams per FTE) = 1500 FTEs x (.625 reams per FTE - .33 reams per FTE)
= 421.5 reams of paper

STEP 4: Determine the average value of the savings/reduction
Average value of a ream of paper in UC contract:$5
$5 x 421.5 reams of paper = $2,107.5

STEP 5: Add the value of the reduction to both the numerator and the denominator of the Green Spend equation for the product category

$$\frac{\text{Green Spend purchase per category} + \$2{,}107.5}{\text{Addressable spend per category} + \$2{,}107.5} \times 100$$

Method 3: Replacement of disposables with reusables

If successful methods have been found to identify reuse numbers where disposables were the standard business as usual, the market value of these disposables may be used in Green Spend calculations. An example of this might be the use of reusable to-go containers at dining locations where reusables are "checked out," so specific numbers of reusables are available.

In these cases, the value of the disposables displaced may be considered Green Spend and added to the numerator and the denominator for the Green Spend calculation. The process for calculating this is as follows:

STEP 1. Determine number of goods displaced.

STEP 2. Determine value of goods displaced per unit.

STEP 3. Calculate total value of goods displaced (number of goods displaced) x (value of goods displaced per unit)

STEP 4. Include the current market value of goods in the numerator and denominator of the Green Spend Calculation.

Method 3 Example:
For this example, a dining operation uses reusable to-go containers and tracks their usage. 500 reusable to-go containers are used in a year.

STEP 1. Determine number of goods displaced

From the example above, 500 to-go containers are displaced

STEP 2. Determine value of goods displaced per unit

Alternative compostable to-go containers cost $0.20 each (on system wide or local contract).

STEP 3. Calculate total value of goods displaced

500 compostable to-go containers x $0.20/container = $100

STEP 4: Add the value of the savings/reduction to both the numerator and the denominator of the Green Spend equation for the product category:

$$\frac{\text{Green Spend purchase per category + \$100}}{\text{Addressable spend per category + \$100}} \times 100$$

EDUCAUSE

Shared Assessments Introduction

Campus IT environments are rapidly changing and the speed of cloud service adoption is increasing. Institutions looking for ways to do more with less see cloud services as a good way to save resources. As campuses deploy or identify cloud services, they must ensure the cloud services are appropriately assessed for managing the risks to the confidentiality, integrity and availability of sensitive institutional information and the PII of constituents. Many campuses have established a cloud security assessment methodology and resources to review cloud services for privacy and security controls. Other campuses don't have sufficient resources to assess their cloud services in this manner. On the vendor side, many cloud services providers spend significant time responding to the individualized security assessment requests made by campus customers, often answering similar questions repeatedly. Both the provider and consumer of cloud services are wasting precious time creating, responding, and reviewing such assessments.

The **Higher Education Community Vendor Assessment Toolkit** (**HECVAT**) attempts to generalize higher education information security and data protections and issues for consistency and ease of use. Some institutions may have specific issues that must be addressed in addition to the general questions sets provided in the toolkit. It is anticipated that the HECVAT will be revised over time to account for changes in services provisioning and the information security and data protection needs of higher education institutions.

The Higher Education Community Vendor Assessment Toolkit:
- Helps higher education institutions ensure that vendor services are appropriately assessed for security and privacy needs, including some that are unique to higher education
- Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through vendor services without increasing risks
- Reduces the burden that service providers face in responding to requests for security assessments from higher education institutions

The Higher Education Community Vendor Assessment Toolkit is a suite of tools built around the original HECVAT (known now as HECVAT - Full) to allow institutions to adopt, implement, and maintain a consistent risk/security assessment program. Tools include:
- **HECVAT - Triage**: Used to initiate risk/security assessment requests - review to determine assessment requirements
- **HECVAT - Full**: Robust questionnaire used to assess the most critical data sharing engagements
- **HECVAT - Lite**: A lightweight questionnaire used to expedite process
- **HECVAT - On-Premise**: Unique questionnaire used to evaluate on-premise appliances and software

The HECVAT (and Toolkit) was created by the Higher Education Information Security Council Shared Assessments Working Group. Its purpose is to provide a starting point for the assessment of vendor provided services and resources. Over time, the Shared Assessments Working Group hopes to create a framework that will establish a community resource where institutions and cloud services providers will share completed Higher Education Cloud Vendor Assessment Tool assessments.

https://www.educause.edu/hecvat
https://www.ren-isac.net/hecvat

(C) EDUCAUSE 2019
This work is licensed under a Creative Commons Attribution-Noncommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).

This Higher Education Cloud Vendor Assessment Toolkit is brought to you by the Higher Education Information Security Council, and members from EDUCAUSE, Internet2, and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).

Proceed to the next tab, Instructions.

Higher Education Community Vendor Assessment Tool - Full - Instructions

Target Audience

These instructions are for vendors interested in providing the institution with a software and/or a service.
This worksheet should not be completed by an institution entity. The purpose of this worksheet is for the vendor to submit robust security safeguard information in regards to the product (software/service) being assessed in the institution's assessment process.

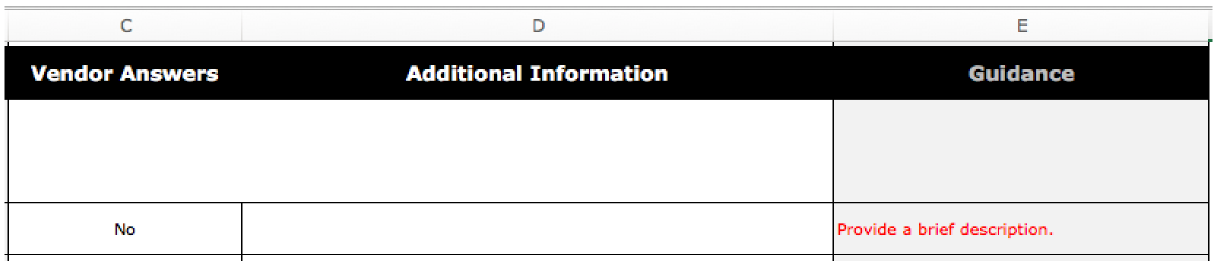
Document Layout

There are five main sections of the Higher Education Community Vendor Assessment Tool - Full, all listed below and outlined in more detail. This document is designed to have the first two sections populated first; after the Qualifiers section is completed it can be populated in any order. Within each section, answer each question top-to-bottom. Some questions are nested and may be blocked out via formatting based on previous answers. Populating this document in the correct order improves efficiency.
Do not overwrite selection values (data validation) in column C of the HECVAT - Full tab.

General Information	This section is self-explanatory; product specifics and contact information. GNRL-01 through GNRL-10 should be populated by the Vendor. GNRL-11 and GNRL-12 are for institution use only.
Qualifiers	Populate this section **completely** before continuing. Answers in this section can determine which sections will be required for this assessment. By answering "No" to Qualifiers, their matched sections become optional and are highlighted in orange.
Documentation	Focused on external documentation, the institution is interested in the frameworks that guide your security strategy and what has been done to certify these implementations.
Company Overview	This section is focused on company background, size, and business area experience.
Safeguards	The remainder of the document consists of various safeguards, grouped generally by section.

In sections where vendor input is required there are only one or two columns that need modification, Vendor Answers and Additional Information, columns C and D respectively (see Figure 1 below). You will see that sometimes C and D are separate and other times are merged. If they are separate, C will be a selectable, drop-down box and any supporting information should be added to column D. If C and D are merged, the question is looking for the answer to be in narrative form. At the far right is a column titled "Guidance". After answering questions, check this column to ensure you have submitted information/documentation to sufficiently answer the question. Use the "Additional Information" column to provide any requested details.

Figure 1:

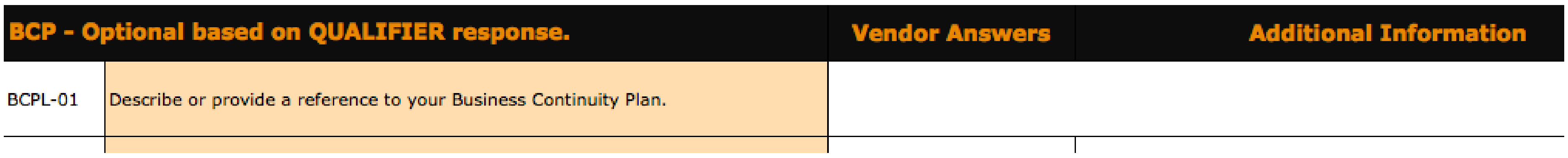


C	D	E
Vendor Answers	**Additional Information**	**Guidance**
No		Provide a brief description.

Optional Safeguards Based on Qualifiers

Not all questions are relevant to all vendors. Qualifiers are used to make whole sections optional to vendors depending on the scope of product usage and the data involved in the engagement being assessed. Sections that become optional have the section titles and questions highlighted in orange (see Figure 2).

Figure 2:



BCP - Optional based on QUALIFIER response.		Vendor Answers	Additional Information
BCPL-01	Describe or provide a reference to your Business Continuity Plan.		

Definitions and Data Zones

Institution	Any school, college, or university using the Higher Education Community Vendor Assessment Tool - Full.
Institution Data Zone	The country/region in which an institution is located, including all laws and regulations in-scope within that country/region.

Vendor Data Zone

The country/region in which a vendor is headquartered and/or serves its products/services, including all laws and regulations in-scope within that country/region.

Customers from different regions may expect vary protections of data (e.g. GDPR), this is the institution Data Zone. Vendors may handle data differently depending on the country or region where data is stored, this is the Vendor Data Zone.
As a vendor, if your security practices vary based on your region of operation, you may want to populate a HECVAT in the context for each security zone (strategy). That said, institutions from different data zones may still use vendor responses from other state Data Zones. If your security practices are the same across all regions of operations, indicate "All" in your Vendor Data Zone.

Example A: If vendor ABC is headquartered and stores data in Canada, and provides services to only customers in Canada, ABC should state "Canada" in both Data Zone fields.
Example B: If vendor ABC is headquartered and stores data in Canada, and additionally provides services to customers in the United Kingdom, ABC may want to assure customers in the United Kingdom that their data is handled properly for their region. In that case, ABC should state "Canada" in the Vendor Data Zone and "United Kingdom" in the institution Data Zone.
Example C: If your security strategy is broad and doesn't fit this statement model, provide a brief summary in each field and the institution's Security Analyst can assess your response.

Data Reporting

To update data in the Report tabs, click Refresh All in the Menu tab. Input provided in the HECVAT tab is assessed a preliminary score pending institution's Security Analyst review.

Proceed to the next tab, HECVAT - Full.

For Institution's Security Analysts

1. Raw vendor answers can be viewed on the **HECVAT - Full** tab.
2. To begin your assessment, review the Analyst Report tab, ensuring that you select the appropriate security standard used in your institution (cell B7) before you begin.
3. Review the Analyst Reference tab for guidance and question/response interpretation.
4. Select compliance states for the outstanding non-compliant or short-answer questions in column G. Once all subjective questions are evaluated and compliance indicated, move to the Summary Report tab.
5. To update the report's data, select Refresh All in the Data menu. Review details in the Summary Report and based on your assessment, follow-up with vendor for clarification(s) or add the Summary Report output to your Institution's reporting documents.

Higher Education Community Vendor Assessment Tool (HECVAT) - Full

Version 2.11

HEISC Shared Assessments Working Group

DATE-01	**Date**	*mm/dd/yyyy*

General Information

In order to protect the Institution and its systems, vendors whose products and/or services will access and/or host institutional data must complete the Higher Education Community Vendor Assessment Toolkit (HECVAT). Throughout this tool, anywhere where the term data is used, this is an all-encompassing term including at least data and metadata. Answers will be reviewed by Institution security analysts upon submittal. This process will assist the institution in preventing breaches of protected information and comply with Institution policy, state, and federal law. This is intended for use by vendors participating in a Third Party Security Assessment and should be completed by a vendor. Review the *Instructions* tab for further guidance.

GNRL-01 through GNRL-08; populated by the Vendor

GNRL-01	Vendor Name	*Vendor Name*
GNRL-02	Product Name	*Product Name and Version Information*
GNRL-03	Product Description	*Brief Description of the Product*
GNRL-04	Web Link to Product Privacy Notice	*http://www.vendor.domain/privacynotice*
GNRL-05	Vendor Contact Name	*Vendor Contact Name*
GNRL-06	Vendor Contact Title	*Vendor Contact Title*
GNRL-07	Vendor Contact Email	*Vendor Contact E-mail Address*
GNRL-08	Vendor Contact Phone Number	*555-555-5555*
GNRL-09	Vendor Data Zone	*See Instructions tab for guidance*
GNRL-10	Institution Data Zone	*See Instructions tab for guidance*

GNRL-11 and GNRL-12; populated by the Institution's Security Office

GNRL-11	Institution's Security Analyst/Engineer	*Institution's Security Analyst/Engineer Name*
GNRL-12	Assessment Contact	*ticket#@yourdomain.edu*

Instructions

Step 1: Complete the *Qualifiers* section first. **Step 2:** Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order. **Step 3:** Submit the completed Higher Education Community Vendor Assessment Toolkit (HECVAT) to the Institution according to institutional procedures.

Qualifiers		Vendor Answers	Additional Information	Guidance
The institution conducts Third Party Security Assessments on a variety of third parties. As such, not all assessment questions are relevant to each party. To alleviate complexity, a "qualifier" strategy is implemented and allows for various parties to utilize this common documentation instrument. **Responses to the following questions will determine the need to answer additional questions below**.				
QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?			
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)			
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)			
QUAL-04	Do you have a Business Continuity Plan (BCP)?			
QUAL-05	Do you have a Disaster Recovery Plan (DRP)?			

QUAL-06	Will data regulated by PCI DSS reside in the vended product?			
QUAL-07	Is your company a consulting firm providing only consultation to the Institution?			
Documentation		**Vendor Answers**	**Additional Information**	**Guidance**
DOCU-01	Have you undergone a SSAE 18 audit?			
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?			
DOCU-03	Have you received the Cloud Security Alliance STAR certification?			
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)			
DOCU-05	Are you compliant with FISMA standards?			
DOCU-06	Does your organization have a data privacy policy?			
Company Overview		**Vendor Answers**	**Additional Information**	**Guidance**
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.			Include circumstances that may involve off-shoring or multi-national agreements.
COMP-02	Describe how long your organization has conducted business in this product area.			Include the number of years and in what capacity.
COMP-03	Do you have existing higher education customers?			
COMP-04	Have you had a significant breach in the last 5 years?			
COMP-05	Do you have a dedicated Information Security staff or office?			
COMP-06	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)			

COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.			Share any details that would help information security analysts assess your product.
Third Parties		**Vendor Answers**	**Additional Information**	**Guidance**
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.			Ensure that all elements of THRD-01 are clearly stated in your response.
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.			If more space is needed to sufficiently answer this question, provide reference to the document or add it as an appendix.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?			Provide sufficient detail for each legal agreement in place.
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.			Robust answers from the vendor improve the quality and efficiency of the security assessment process.
Consulting		**Vendor Answers**	**Additional Information**	**Guidance**
CONS-01	Will the consulting take place on-premises?			
CONS-02	Will the consultant require access to Institution's network resources?			
CONS-03	Will the consultant require access to hardware in the Institution's data centers?			
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?			
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?			
CONS-06	Will any data be transferred to the consultant's possession?			
CONS-07	Is it encrypted (at rest) while in the consultant's possession?			
CONS-08	Will the consultant need remote access to the Institution's network or systems?			
CONS-09	Can we restrict that access based on source IP address?			

Application/Service Security		Vendor Answers	Additional Information	Guidance
APPL-01	Do you support role-based access control (RBAC) for end-users?			
APPL-02	Do you support role-based access control (RBAC) for system administrators?			
APPL-03	Can employees access customer data remotely?			
APPL-04	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?			
APPL-05	Does the system provide data input validation and error messages?			
APPL-06	Do you employ a single-tenant environment?			
APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?			List all operating systems and the roles that are fulfilled by each.
APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?			
APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.			Describe the products and how they will be implemented.
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.			Ensure that all parts of APPL-10 are clearly stated in your response. Submit architecture diagrams along with this fully-populated HECVAT.
APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)			
APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).			Include both end-user and administrative features and functions.
APPL-13	Are there any OS and/or web-browser combinations that are not currently supported?			
APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?			

APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.		Include a detailed description of how security administration and system administration authority is separated, controls are verified, and logs are reviewed regularly to ensure appropriate use
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)		Ensure that all parts of APPL-16 are clearly stated in your response.
APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).		Ensure that all parts of APPL-18 are clearly stated in your response. The examples given are not exhaustive - elaborate as necessary.

Authentication, Authorization, and Accounting		Vendor Answers	Additional Information	Guidance
AAAI-01	Can you enforce password/passphrase aging requirements?			
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?			
AAAI-03	Does the system have password complexity or length limitations and/or restrictions?			
AAAI-04	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?			
AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)			
AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?			
AAAI-07	Are user account passwords/passphrases visible in administration modules?			
AAAI-08	Are user account passwords/passphrases stored encrypted?			
AAAI-09	Does your *application* and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)			
AAAI-10	Does your *application* support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?			
AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?			
AAAI-12	Does the *system* (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?			
AAAI-13	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?			
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?			

AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?			
AAAI-16	Describe or provide a reference to the a) system capability to **log** security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.			Ensure that all elements of AAAI-16 are clearly stated in your response.
AAAI-17	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).			Ensure that all elements of AAAI-17 are clearly stated in your response.
Business Continuity Plan		**Vendor Answers**	**Additional Information**	**Guidance**
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).			Provide a valid URL to your current BCP or submit it along with this fully-populated HECVAT.
BCPL-02	May the Institution review your BCP and supporting documentation?			
BCPL-03	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?			
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?			
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?			
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?			
BCPL-07	Has your BCP been tested in the last year?			
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?			
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?			
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?			
BCPL-11	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?			
BCPL-12	Is this product a core service of your organization, and as such, the top priority during business continuity planning?			
Change Management		**Vendor Answers**	**Additional Information**	**Guidance**
CHNG-01	Do you have a documented and currently followed change management process (CMP)?			

CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.			Ensure that all parts of CHNG-02 are clearly stated in your response.
CHNG-03	Will the Institution be notified of major changes to your environment that could impact the Institution's security posture?			
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?			
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)			Ensure that all relevant details pertaining to CHNG-05 are clearly stated in your response.
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.			Ensure that all parts of CHNG-06 are clearly stated in your response.
CHNG-07	Does the system support client customizations from one release to another?			
CHNG-08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?			
CHNG-09	Do you have a release schedule for product updates?			
CHNG-10	Do you have a technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed?			
CHNG-11	Is Institution involvement (i.e. technically or organizationally) required during product updates?			
CHNG-12	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?			
CHNG-13	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?			
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?			
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?			
Data		**Vendor Answers**	**Additional Information**	**Guidance**

DATA-01	Do you physically and logically separate Institution's data from that of other customers?			
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?			
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)			
DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?			
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?			
DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)			
DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?			Ensure that all parts of DATA-07 are clearly stated in your response.
DATA-08	At the completion of this contract, will data be returned to the institution?			
DATA-09	Will the institution's data be available within the system for a period of time at the completion of this contract?			
DATA-10	Can the institution extract a full backup of data?			
DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?			
DATA-12	Are these rights retained even through a provider acquisition or bankruptcy event?			
DATA-13	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?			
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.			If your strategy uses different processes for services and data, ensure that all strategies are clearly stated and supported.
DATA-15	Are backup copies made according to pre-defined schedules and securely stored and protected?			
DATA-16	How long are data backups stored?			If your backup strategy uses varying periods, ensure that each strategy is clearly stated and supported.
DATA-17	Are data backups encrypted?			
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)			

DATA-19	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?			
DATA-20	Are you performing off site backups? (i.e. digitally moved off site)			
DATA-21	Are physical backups taken off site? (i.e. physically moved off site)			
DATA-22	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?			
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?			
DATA-24	Does the process described in DATA-23 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?			
DATA-25	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?			
DATA-26	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?			
DATA-27	Will you handle data in a FERPA compliant manner?			
DATA-28	Is any institution data visible in system administration modules/tools?			
Database		**Vendor Answers**	**Additional Information**	**Guidance**
DBAS-01	Does the database support encryption of specified data elements in storage?			
DBAS-02	Do you currently use encryption in your database(s)?			
Datacenter		**Vendor Answers**	**Additional Information**	**Guidance**
DCTR-01	Does your company own the physical data center where the Institution's data will reside?			
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?			
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?			
DCTR-04	Do any of your servers reside in a co-located data center?			
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?			

DCTR-06	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?			
DCTR-07	Select the option that best describes the network segment that servers are connected to.			Provide a general summary of the implemented networking strategy.
DCTR-08	Does this data center operate outside of the Institution's Data Zone?			
DCTR-09	Will any institution data leave the Institution's Data Zone?			
DCTR-10	List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the Institution's Data Zone).			Ensure that all parts of DCTR-10 are clearly stated in your response.
DCTR-11	Are your primary and secondary data centers geographically diverse?			
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?			
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?			Review the Uptime Institute's level/tier direction provided on their website if you need addition information to answer DCTR-13.
DCTR-14	Is the service hosted in a high availability environment?			
DCTR-15	Is redundant power available for all datacenters where institution data will reside?			
DCTR-16	Are redundant power strategies tested?			
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.			Ensure that all parts of DCTR-17 are clearly stated in your response.
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.			State the ISP provider(s) in addition to the number of ISPs that provide connectivity.
DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?			
Disaster Recovery Plan		**Vendor Answers**	**Additional Information**	**Guidance**
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).			Provide a valid URL to your current DRP or submit it along with this fully-populated HECVAT.
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?			
DRPL-03	Can the Institution review your DRP and supporting documentation?			
DRPL-04	Are any disaster recovery locations outside the Institution's Data Zone?			

DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?			
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?			
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?			
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?			
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)			Ensure that all elements of DRPL-09 are clearly stated in your response.
DRPL-10	Has the Disaster Recovery Plan been tested in the last year? Please provide a summary of the results in Additional Information (including actual recovery time).			
DRPL-11	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?			
DRPL-12	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?			
DRPL-13	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?			

Firewalls, IDS, IPS, and Networking		Vendor Answers	Additional Information	Guidance
FIDP-01	Are you utilizing a web application firewall (WAF)?			
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?			
FIDP-03	State and describe who has the authority to change firewall rules?			Ensure that all parts of FIDP-03 are clearly stated in your response.
FIDP-04	Do you have a documented policy for firewall change requests?			
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?			
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?			
FIDP-07	Do you employ host-based intrusion detection?			
FIDP-08	Do you employ host-based intrusion prevention?			
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?			

FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?			
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?			In addition to stating your intrusion monitoring strategy, provide a brief summary of its implementation.
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?			
Mobile Applications		**Vendor Answers**	**Additional Information**	**Guidance**
MAPP-01	On which mobile operating systems is your software or service supported?			Ensure that all supported operating systems are listed - be sure to provide version number, where relevant.
MAPP-02	Describe or provide a reference to the application's architecture and functionality.			Ensure that all elements of MAPP-02 are clearly stated in your response. (i.e. (architecture AND functionality are
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?			
MAPP-04	Does the application store, process, or transmit critical data?			
MAPP-05	Is Institution's data encrypted in transport?			
MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)			
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?			
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?			
MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?			
MAPP-10	Has the application been tested for vulnerabilities by a third party?			
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?			Ensure that all elements of MAPP-11 are clearly stated in your response.
Physical Security		**Vendor Answers**	**Additional Information**	**Guidance**
PHYS-01	Does your organization have physical security controls and policies in place?			
PHYS-02	Are employees allowed to take home Institution's data in any form?			
PHYS-03	Are video monitoring feeds retained?			
PHYS-04	Are video feeds monitored by datacenter staff?			

PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?			
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**	**Guidance**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?			
PPPR-02	Do you have a documented patch management process?			
PPPR-03	Can you accommodate encryption requirements using open standards?			
PPPR-04	Have your developers been trained in secure coding techniques?			
PPPR-05	Was your application developed using secure coding techniques?			
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?			
PPPR-07	Do you have software testing processes (dynamic or static) that are established and followed?			
PPPR-08	Are information security principles designed into the product lifecycle?			
PPPR-09	Do you have a documented systems development life cycle (SDLC)?			
PPPR-10	Do you have a formal incident response plan?			
PPPR-11	Will you comply with applicable breach notification laws?			
PPPR-12	Will you comply with the Institution's IT policies with regards to user privacy and data protection?			
PPPR-13	Is your company subject to Institution's Data Zone laws and regulations?			
PPPR-14	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?			
PPPR-15	Do you require new employees to fill out agreements and review policies?			

PPPR-16	Do you have documented information security policy?			
PPPR-17	Do you have an information security awareness program?			
PPPR-18	Is security awareness training mandatory for all employees?			
PPPR-19	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?			
PPPR-20	Do you have documented, and currently implemented, internal audit processes and procedures?			
Product Evaluation		**Vendor Answers**	**Additional Information**	**Guidance**
PROD-01	Do you incorporate customer feedback into security feature requests?			
PROD-02	Can you provide an evaluation site to the institution for testing?			
Quality Assurance		**Vendor Answers**	**Additional Information**	**Guidance**
QLAS-01	Provide a general summary of your Quality Assurance program.			Provide a valid URL to your Quality Assurance program or submit it along with this fully-populated HECVAT.
QLAS-02	Do you comply with ISO 9001?			
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?			
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?			
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?			
Systems Management & Configuration		**Vendor Answers**	**Additional Information**	**Guidance**
SYST-01	Are systems that support this service managed via a separate management network?			
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)			
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?			
SYST-04	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?			

Vulnerability Scanning		Vendor Answers	Additional Information	Guidance
VULN-01	Are your *applications* scanned externally for vulnerabilities?			
VULN-02	Have your applications had an external vulnerability assessment in the last year?			
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?			
VULN-04	Are your *systems* scanned externally for vulnerabilities?			
VULN-05	Have your systems had an external vulnerability assessment in the last year?			
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.			Ensure that all elements of VULN-06 are clearly stated in your response.
VULN-07	Will you provide results of security scans to the Institution?			
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).			Ensure that all elements of VULN-08 are clearly stated in your response.
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?			

HIPAA		Vendor Answers	Additional Information	Guidance
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?			Refer to HIPAA regulations documentation for supplemental guidance in this section.

HIPA-08	Have you identified areas of risks?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-09	Have you taken actions to mitigate the identified risks?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-12	Does your application lock-out an account after a number of failed login attempts?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-16	Does your application provide the ability to define user access levels?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-18	Does your application support varying levels of access to records based on user ID?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-19	Is there a limit to the number of groups a user can be assigned?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-23	How long does the application keep access/change logs?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-24	Can the application logs be archived?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-25	Can the application logs be saved externally?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?			Refer to HIPAA regulations documentation for supplemental guidance in this section.

HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-28	Have the policies/plans mentioned above been tested?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-29	Can you provide a HIPAA compliance attestation document?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-30	Are you willing to enter into a Business Associate Agreement (BAA)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
HIPA-31	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?			Refer to HIPAA regulations documentation for supplemental guidance in this section.
PCI DSS		**Vendor Answers**	**Additional Information**	**Guidance**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-04	Are you classified as a service provider?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-05	Are you on the list of VISA approved service providers?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-08	What payment processors/gateways does the system support?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-09	Can the application be installed in a PCI DSS compliant manner ?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-10	Is the application listed as an approved PA-DSS application?			Refer to PCI DSS Security Standards for supplemental guidance in this section
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?			
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.			Refer to PCI DSS Security Standards for supplemental guidance in this section

Higher Education Community Vendor Assessment Tool (HECVAT) - Full - Standards Crosswalk

HEISC Shared Assessments Working Group

Qualifiers		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	CSC 13	Discovery	18.1.1	ID.GV-3	ID.GV-3	RA-2	
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)	CSC 18					IA-2, IA-3, CM-3, SI-2	
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)	CSC 13			ID.AM-6, PR.AT-3	ID.AM-6, PR.AT-3		12.8
QUAL-04	Do you have a Business Continuity Plan (BCP)?	CSC 10		17.1.2	PR.IP-9	PR.IP-9	AU-7, AU-9, IR-4	12.1
QUAL-05	Do you have a Disaster Recovery Plan (DRP)?	CSC 10		17.1.2	PR.IP-9	PR.IP-9	CA-5, PL-2	12.1
QUAL-06	Will data regulated by PCI DSS reside in the vended product?	CSC 13		18.1.1	ID.GV-3	ID.GV-3	RA-2	PCI Scope, Discovery
QUAL-07	Is your company a consulting firm providing only consultation to the Institution?	CSC 14						PCI Scope

Documentation		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
DOCU-01	Have you undergone a SSAE 18 audit?			15.2.1			SA-9	
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?			15.2.1			PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	
DOCU-03	Have you received the Cloud Security Alliance STAR certification?			15.2.1			PE-2, PE-3, PE-5, PE-11, PE-13, PE-14, SA-9	
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)			18.1.1			SA-9	12.1, Scope
DOCU-05	Are you compliant with FISMA standards?			18.1.1			SA-9	
DOCU-06	Does your organization have a data privacy policy?		§164.308(a)(1)(i)	18.1.4	ID.GV-3	ID.GV-3	SA-9	

Company Overview		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.							12.8
COMP-02	Describe how long your organization has conducted business in this product area.							12.8
COMP-03	Do you have existing higher education customers?			15.2.1				12.8
COMP-04	Have you had a significant breach in the last 5 years?							
COMP-05	Do you have a dedicated Information Security staff or office?			15.2.1				12.8, 12.5
COMP-06	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)			14.2.1			SA-3, SA-15, SC-2, PM-2, PM-10, SI-5,PM-3	12.8

COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.			15.2.1				12.8
Third Parties		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.	CSC 13		15.1.3	ID.AM-6, PR-AT-3	3.8.2	MP-2, RA-3	12.8
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	CSC 13		15.1.3	ID.AM-6, PR-AT-3	3.8.2		12.8
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	CSC 13		15.1.3	ID.GV-3		PS-3	12.8
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.			15.1.3	ID.AM-6, PR.AT-3		PS-5	12.8
Consulting - Optional based on QUALIFIER response.		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
CONS-01	Will the consulting take place on-premises?			15.2.1	ID.AM-6, PR.AT-3			
CONS-02	Will the consultant require access to Institution's network resources?	CSC 14		9.1.2	ID.AM-6, PR.AT-3	3.1.2, 3.1.3	AC-4	
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	CSC 14		9.2.6	ID.AM-6, PR.AT-3	3.1.2		
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	CSC 14			ID.AM-6, PR.AT-3			
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	CSC 13		18.1.1	ID.AM-6, PR.AT-3			
CONS-06	Will any data be transferred to the consultant's possession?	CSC 13		9	ID.AM-6, PR.AT-3	3.8.2	MP-2	
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	CSC 13		10	ID.AM-6, PR.AT-3	3.1.2, 3.1.19, 3.8.2	MP-2	
CONS-08	Will the consultant need remote access to the Institution's network or systems?	CSC 14		9	ID.AM-6, PR.AT-3			
CONS-09	Can we restrict that access based on source IP address?			9	ID.AM-6, PR.AT-3			
Application/Service Security		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
APPL-01	Do you support role-based access control (RBAC) for end-users?	CSC 18			ID.AM-5			
APPL-02	Do you support role-based access control (RBAC) for system administrators?	CSC 2, CSC 3		11.2.6	ID.AM-5			
APPL-03	Can employees access customer data remotely?	CSC 14		6.2	PR.AC-3, PR.MA-2	3.1.2	AC-17; NIST SP 800-46	7.x
APPL-04	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?	CSC16		9.1.1	PR.AC-4, PR.PT-3	3.4.9	CM-11	7.x
APPL-05	Does the system provide data input validation and error messages?	CSC 18			ID.AM-5			
APPL-06	Do you employ a single-tenant environment?	CSC 12		6.2	PR.PT-3	3.1.12, 3.1.13, 3.1.14, 3.1.14, 3.1.15, 3.1.8, 3.1.20, 3.7.5, 3.8.2, 3.13.7	AC-3, CM-7; NIST SP 800-46	

APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?	CSC 2		12.5.1	PR.PT-3		AC-17; NIST SP 800-46	
APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?			16				12.8, 4.2
APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.	CSC 2		12.5.1	ID.AM-2			
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.	CSC 2		12.1.1	ID.AM-1, ID.AM-2, ID.AM-4		CA-9, SC-4	2.4
APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)	CSC 13		12.1.4				
APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	CSC 7		12.1.1				
APPL-13	Are there any OS and/or web-browser combinations that are not currently supported?	CSC 7		12.5.1				
APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?	CSC 2						
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	CSC 14		9.2.3, 12.1.4	PR.AC-4, PR.PT-3	3.1.4	AC-5	12.x
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)	CSC 5		9.2	PR.AC-4, PR.PT-3	3.1.1, 3.1.5, 3.1.6, 3.7.1, 3.7.2	AC-2, AC-3, AC-6, MA-2, MA-3	7.x, 8.x
APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).	CSC 14		9.1.1	PR.AC-4	3.1.2		

Authentication, Authorization, and Accounting		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
AAAI-01	Can you enforce password/passphrase aging requirements?	CSC 16		9.2.3, 9.3.1, 9.4.3	PR.AC-1	3.5.6	IA-4	8.x
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?	CSC 16		9.2.3, 9.3.1, 9.4.3	PR.AC-1	3.5.7	IA-5(1)	8.x
AAAI-03	Does the system have password complexity or length limitations and/or restrictions?	CSC 16		9.2.3, 9.3.1, 9.4.3	PR.AC-1			8.x
AAAI-04	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?	CSC 16		9.2.3, 9.3.1, 9.4.3	PR.AC-1	3.5.5, 3.5.8	IA-4	2.1, 8.x
AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)	CSC 16		9.1.1, 9.2.3, 9.3.1, 9.4.3	PR.AC-1	3.5.1	IA-2, IA-5	8.x
AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?	CSC 16		9				2.1, 8.x
AAAI-07	Are user account passwords/passphrases visible in administration modules?	CSC 16		9	PR.AC-1			8.x
AAAI-08	Are user account passwords/passphrases stored encrypted?	CSC 16		9	PR.AC-1	3.5.10	IA-5(1)	8.x
AAAI-09	Does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	CSC 16		9	PR.AC-4	3.5.2, 3.5.3	IA-5	8.x
AAAI-10	Does your application support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?	CSC 16		9.4.3	PR.AC-1, PR.AC-4			

AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?	CSC 16		9	PR.AC-1, PR.AC-4			8.x
AAAI-12	Does the system (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	CSC 16		9.4.3	PR.AC-1, PR.AC-4			
AAAI-13	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?	CSC 16			PR.AC-1, PR.AC-4			
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?	CSC 16			PR.AC-1, PR.AC-4	3.1.1		8.x
AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	CSC 6		12.4	PR.PT-1	3.1.7, 3.3.1	AC-6(1,3,9), AU-2, AU-2(3), AU-3, AU-7, AU-9(4), AU-12, NIST 800-92	10.1, 10.2, 10.3, 10.5, 10.6, 10.7
AAAI-16	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.	CSC 6		12.4	PR.PT-1	3.1.7, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.3, 3.7.1, 3.7.6, 3.10.4, 3.10.5	AU-2(3), AU-6, AU-12, AC-6(9), CM-3, MA-2, MA-5, PE-3	10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 9.x
AAAI-17	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	CSC 6		12.4	PR.PT-1	3.3.8, 3.3.9	AU-9	10.7
Business Continuity Plan		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).	CSC 10		17.1.1	PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
BCPL-02	May the Institution review your BCP and supporting documentation?	CSC 10			PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	
BCPL-03	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	CSC 10		17.1.1	PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	CSC 10		17	PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?	CSC 10		17.1.2	PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	CSC 10		17.1.2	PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
BCPL-07	Has your BCP been tested in the last year?	CSC 10		17.1.3	PR.IP-9	3.12.2	AU-7, AU-9, IR-4, AC-5, CP-4, CP-10; NIST SP 800-34	
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	CSC 10		7.2.2, 17.1.3	PR.IP-9	3.2.1, 3.2.2	AT-3, AC-5, CP-4, CP-10; NIST SP 800-34	12.x
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?	CSC 10		7.2.2, 16.1.1, 17.1.3	PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.x
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?	CSC 10		17.2.1	PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.1
BCPL-11	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	CSC 10		17.1.3	PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.1
BCPL-12	Is this product a core service of your organization, and as such, the top priority during business continuity planning?	CSC 10			PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.1
Change Management		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
CHNG-01	Do you have a documented and currently followed change management process (CMP)?	CSC 10		12.1.2	PR.IP-3	3.4.3, 3.4.4	CM-3, CM-4, CM-5	6.4, 6.4.5, 6.4.5.1, 6.4.5.2
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.	CSC 10		12.1.2	PR.IP-3, PR.DS-7	3.4.3, 3.4.4, 3.4.5	CM-3, CM-4, CM-5	6.4, 6.4.5, 6.4.5.1, 6.4.5.2
CHNG-03	Will the Institution be notified of major changes to your environment that could impact the Institution's security posture?	CSC 10		12.1.2			CM-3, CM-4, CM-5	6.4, 12.8, 12.9

CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	CSC 10					CM-3, CM-4, CM-5	12.1
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)	CSC 2					CM-3, CM-4, CM-5	12.1, 12.8
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.	CSC 2					CM-3, CM-4, CM-5	
CHNG-07	Does the system support client customizations from one release to another?	CSC 10					CM-3, CM-4, CM-5	
CHNG-08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?	CSC 2		12.1.1	PR.DS-6	3.4.4	CM-3, CM-4, CM-5	12.1
CHNG-09	Do you have a release schedule for product updates?	CSC 10				3.14.4	CM-3, CM-4, CM-5	
CHNG-10	Do you have a technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed?	CSC 2					CM-3, CM-4, CM-5	
CHNG-11	Is Institution involvement (i.e. technically or organizationally) required during product updates?						CM-3, CM-4, CM-5	
CHNG-12	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	CSC 2		12.6.1			CM-3, CM-4, CM-5	12.1, 12.8, 6.2
CHNG-13	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	CSC 13	§164.308(a)(1)(ii)(B)	12.6.1			CM-3, CM-4, CM-5	12.2, 12.8
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	CSC 10					CM-3, CM-4, CM-5	12.1, 12.2, 12.8
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	CSC 10		12.1.2	PR.IP-3		CM-3, CM-4, CM-5	12.10, 12.8, 6.4

Data		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
DATA-01	Do you physically and logically separate Institution's data from that of other customers?	CSC 12			PR.AC-2, PR.IP-5	3.1.3, 3.8.1	AC-4, MP-2, MP-4	12.8
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	CSC 12			PR.AC-2, PR.IP-5	3.1.22	AC-22	12.8, 9.x
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)	CSC 13		10.1.1	PR.DS-2			12.8, 4.1
DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	CSC 13		8.2.3, 10.1.1	PR.DS-1	3.1.19, 3.8.1	MP-2, AC-19(5)	12.8
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	CSC 13		8.2.3, 10.1.1		3.8.6, 3.13.11		12.1
DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)	CSC 13		13.2	PR.DS-2		PE-2, PE-3, PE-5, MP-5	12.8, 4.1
DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	CSC 1				3.8.1	MP-2	12.8, 9.x
DATA-08	At the completion of this contract, will data be returned to the institution?	CSC 13		8.1.4		3.8.1	MP-2	12.8
DATA-09	Will the institution's data be available within the system for a period of time at the completion of this contract?	CSC 13		8.1.4				12.8
DATA-10	Can the institution extract a full backup of data?			12.3.1				12.8

DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	CSC 13		8.1.2		3.8.1		12.8
DATA-12	Are these rights retained even through a provider acquisition or bankruptcy event?	CSC 13		8.1.2		3.8.2		12.8
DATA-13	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	CAC 13		8.1.2		3.8.1		12.8
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	CSC 10		12.3.1	PR.IP-4	3.8.9	CP-9	9.x
DATA-15	Are backup copies made according to pre-defined schedules and securely stored and protected?	CSC 10		12.3.1	PR.IP-4	3.8.9	CP-9	12.8
DATA-16	How long are data backups stored?	CSC 10		12.3.1	PR.IP-4	3.8.9	CP-9	
DATA-17	Are data backups encrypted?	CSC 10		12.3.1	PR.DS-1, PR.IP-4	3.8.9	CP-9	
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)	CSC 10		10.1.2		3.13.10	SC-28, SC-13, FIPS PUB 140-2	
DATA-19	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	CSC 10		12.3.1	ID.AM-1, ID.AM-2, PR.IP-9	3.8.9	CP-9	
DATA-20	Are you performing off site backups? (i.e. digitally moved off site)	CSC 10		12.3.1	PR.IP-4	3.8.1, 3.8.9	CP-9	9.x
DATA-21	Are physical backups taken off site? (i.e. physically moved off site)	CSC 10		12.3.1	PR.IP-4	3.8.1, 3.8.5, 3.8.9	CP-9, MP-5	9.x
DATA-22	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?	CSC 13		12.3.1		3.8.9	CP-9, MP-5	12.8
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?	CSC 13		8.3.1	PR.DS-3	3.7.1, 3.7.2, 3.8.3	CP-9 MP-6, NIST SP 800-60, NIST SP 800-88, AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2, MA-3, MP-6	9.x
DATA-24	Does the process described in DATA-23 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	CSC 13		8.3.1, 18.1.1	PR.DS-3	3.7.3, 3.8.3,	AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2	
DATA-25	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?	CSC 13		8.3.1, 18.1.1	PR.DS-3, ID.GV-3	3.7.3, 3.8.3,	SI-12, AC-2, AC-6, IA-4, PM-2, PM-10, SI-5, MA-2	
DATA-26	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	CSC 13		8.3.1, 18.1.1	PR.DS-3	3.8.1, 3.8.2	AC-2, AC-6, IA-4, PM-2, PM-10, SI-5	12.8, 9.x
DATA-27	Will you handle data in a FERPA compliant manner?	CSC 13		18.1.1	ID.GV-3			
DATA-28	Is any institution data visible in system administration modules/tools?	CSC 13, CSC 14		14.2.5	PR.AC-4			
Database		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
DBAS-01	Does the database support encryption of specified data elements in storage?	CSC 13		10.1.1	PR.DS-1			
DBAS-02	Do you currently use encryption in your database(s)?	CSC 13		10.1.1	PR.DS-1, PR.DS-2			
Datacenter		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
DCTR-01	Does your company own the physical data center where the Institution's data will reside?	CSC 14		11.1.1	PR.AC-2, PR.IP-5			12.8, 9.x
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?	CSC 13		11.1.1				
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?	CSC 3		17.2.1				
DCTR-04	Do any of your servers reside in a co-located data center?	CSC 3, CSC 14					AC-4	12.8
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	CSC 3, CSC 14		13.1.2	PR.AC-2			9.x
DCTR-06	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	CSC 14		11.1.1, 11.1.2	PR.AC-2	3.8.1, 3.8.2		9.x

DCTR-07	Select the option that best describes the network segment that servers are connected to.	CSC 9			PR.AC-5	3.1.3		
DCTR-08	Does this data center operate outside of the Institution's Data Zone?	CSC 12		18.1.1				12.8
DCTR-09	Will any institution data leave the Institution's Data Zone?	CSC 12		18.1.1				12.9
DCTR-10	List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the Institution's Data Zone).	CSC 12		11.2.1				12.8
DCTR-11	Are your primary and secondary data centers geographically diverse?	CSC 10		11.1.4				12.8
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?	CSC 12		18.1.1				12.8
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?			17.1.1				
DCTR-14	Is the service hosted in a high availability environment?	CSC 10		17.1.1	PR.DS-4			
DCTR-15	Is redundant power available for all datacenters where institution data will reside?			17.2.1	PR.DS-4			
DCTR-16	Are redundant power strategies tested?			17.1.3	PR.DS-4			
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.			17.2.1			PE-2, PE-3, PE-5, PE-11, PE-13, PE-14	
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.	CSC 10		17.2.1	PR.DS-4		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14	12.8
DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	CSC 13		17.2.1	PR.DS-4		PE-2, PE-3, PE-5, PE-11, PE-13, PE-14	12.8
Disaster Recovery Plan		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	CSC 10		17.1.1	PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	CSC 10		16.1.1, 17.1.1	PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
DRPL-03	Can the Institution review your DRP and supporting documentation?	CSC 10			PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
DRPL-04	Are any disaster recovery locations outside the Institution's Data Zone?	CSC 10, CSC 12		17.1.1	PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.8
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?	CSC 10		17.2.1	PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	CSC 10		17.1.3	PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	CSC 10			PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	CSC 10		17.1.2	PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	CSC 10		17.1.3	PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	
DRPL-10	Has the Disaster Recovery Plan been tested in the last year? Please provide a summary of the results in Additional Information (including actual recovery time).	CSC 10		17.1.3	PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	
DRPL-11	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?	CSC 10		7.1.3	PR.IP-9		AC-5, CP-4, CP-10; NIST SP 800-34	12.8
DRPL-12	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	CSC 10		17.1.1	PR.IP-9	3.12.2	AC-5, CP-4, CP-10; NIST SP 800-34	
DRPL-13	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?					3.6.2	AC-5, CP-4, CP-10; NIST SP 800-34	12.8

Firewalls, IDS, IPS, and Networking		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
FIDP-01	Are you utilizing a web application firewall (WAF)?	CSC 9		13.1.1	PR.DS-5			1.1
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?	CSC 9		13.1.1	PR.DS-5			1.1
FIDP-03	State and describe who has the authority to change firewall rules?	CSC 9		13	PR.AC-5			1.1
FIDP-04	Do you have a documented policy for firewall change requests?	CSC 9		12.1.2	PR.AC-5			1.1
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?	CSC 19		13.1.2	DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?	CSC 19		13.1.2	DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
FIDP-07	Do you employ host-based intrusion detection?	CSC 19		13.1.2	DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
FIDP-08	Do you employ host-based intrusion prevention?	CSC 19		13.1.2	DE.CM-1	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?	CSC 19		12.4.1		3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.5
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?	CSC 19		12.4.1	DE.CM-1, DE.CM-2, DE.CM-7	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?	CSC 6, CSC 19		12.4.1	DE.CM-1, DE.CM-2, DE.CM-7	3.6.1, 3.14.6, 3.14.7	IR-2, IR-4, IR-5	11.4, 12.8
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	CSC 6		12.4.1	DE.AE-1, DE.CM-1, PR.PT-4	3.3.1	AU-2	1.1, 10.8, 10.6, 10.3, 10.2, 11.4

Mobile Applications		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
MAPP-01	On which mobile operating systems is your software or service supported?	CSC 18						
MAPP-02	Describe or provide a reference to the application's architecture and functionality.	CSC 3			DE.CM-7			
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?	CSC 18			DE.CM-7			
MAPP-04	Does the application store, process, or transmit critical data?	CSC 13, CSC 18		8.2.1; 8.2.3	DE.CM-7, PR.DS-2			
MAPP-05	Is Institution's data encrypted in transport?	CSC 13		8.2.3	DE.CM-7, PR.DS-2	3.1.19	AC-19(5)	4.1
MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)	CSC 14		8.2.3	DE.CM-7, PR.DS-1			
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?	CSC 16		9.4.2				
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?	CSC 16						
MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?	CSC 18		14.2.1	DE.CM-7			
MAPP-10	Has the application been tested for vulnerabilities by a third party?	CSC 18		12.7.1, 18.2.1	DE.CM-7, DE.CM-8, ID.RA-1			
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?	CSC 18		12.7.1, 18.2.1	DE.CM-7, DE.CM-8, ID.RA-1			

Physical Security		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
PHYS-01	Does your organization have physical security controls and policies in place?	CSC 3		11.1.1	PR.AC-2, PR.AT-5, PR.IP-5, DE.CM-2	3.8.2, 3.10.1, 3.10.2, 3.10.5, 3.10.6, 3.12.1	MP-4, PE-2, PE-5, PE-6, PE-17	9.x
PHYS-02	Are employees allowed to take home Institution's data in any form?	CSC 13		8.2.3	PR.AC-2, PR.AC-4, PR.DS-1, PR.DS-3, PR.DS-5	3.8.1, 3.8.5, 3.8.7	MP-2, MP-5, MP-7	12.1, 9.x
PHYS-03	Are video monitoring feeds retained?	CSC 3		11.1.2, 11.1.3	DE.CM-2	3.10.2	PE-6	9.x
PHYS-04	Are video feeds monitored by datacenter staff?	CSC 3		11.1.2, 11.1.3	DE.CM-2	3.10.2	PE-6	9.x
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?	CSC 14		11.1.2	PR.DS-3	3.7.3, 3.8.1, 3.8.5, 3.8.7, 3.10.3	MP-2, MP-5, MP-7	9.x

Policies, Procedures, and Processes		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?			5.1.1	ID.GV-2	3.9.1, 3.9.2	PM-2, PM-10, SI-5, CA-5, PM-1	12.4, 12.5
PPPR-02	Do you have a documented patch management process?	CSC 4		12.6.1	PR.IP-12		CA-5, PM-1	6.4.5
PPPR-03	Can you accommodate encryption requirements using open standards?	CSC 13		10.1.1, 18.1.5			CA-5, PM-1	
PPPR-04	Have your developers been trained in secure coding techniques?	CSC 4, CSC 17		14.2.1			CA-5, PM-1	12.6, 6.5
PPPR-05	Was your application developed using secure coding techniques?	CSC 4		14.2.1			CA-5, PM-1	6.3
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?	CSC 4		14.2.1, 14.2.5, 14.2.8	DE.CM-8, RS.MI-3		CA-5, PM-1	6.3.2
PPPR-07	Do you have software testing processes (dynamic or static) that are established and followed?	CSC 4		14.2.8	PR.DS-7	3.12.2	CA-5, PM-1	6.3.2, 6.4.5.3
PPPR-08	Are information security principles designed into the product lifecycle?	CSC 4		14.2.1		3.13.2	CA-5, PM-1	6.3, 6.3.1
PPPR-09	Do you have a documented systems development life cycle (SDLC)?	CSC 4		14.2.1	PR.IP-2		CM-3, SA-15, SA-3, SA-8, SC-2, CA-5, PM-1	6.3.2
PPPR-10	Do you have a formal incident response plan?	CSC 19		16.1.5	PR.IP-9	3.6.1, 3.12.2	CA-5, PM-1, IR-4, IR-5, IR-7, IR-8	12.10, 12.8, 12.9
PPPR-11	Will you comply with applicable breach notification laws?	CSC 19		18.1.1	ID.GV-3	3.6.2,	CA-5, PM-1, IR-4, IR-5, IR-6, IR-7, IR-8	12.8
PPPR-12	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	CSC 13		18.1.1		3.6.2	CA-2, SA-15, CA-5, PM-1, IR-4, IR-5, IR-6, R-7, IR-8	12.8
PPPR-13	Is your company subject to Institution's Data Zone laws and regulations?	CSC 19		18.1.1	ID.GV-3		CA-5, PM-1	
PPPR-14	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	CSC 5		7.1.1	PR.IP-11	3.9.1	CA-5, PM-1, PS-3	12.7
PPPR-15	Do you require new employees to fill out agreements and review policies?	CSC 17		7.1.2	PR.IP-11		CA-5, PM-1	12.6, 7.x, 8.x, 9.x
PPPR-16	Do you have documented information security policy?	CSC 17	§164.308(a)(1)(i)	5.1.1	ID.GV-3		CA-5, PM-1	12.1, 5.4 (?)
PPPR-17	Do you have an information security awareness program?	CSC 17	§164.308(a)(5)(i)	7.2.2	PR.AT-1	3.2.1	AT-2, CA-5, PM-1	12.6
PPPR-18	Is security awareness training mandatory for all employees?	CSC 17	§164.308(a)(5)(i)	7.2.2	PR.AT-1	3.2.1, 3.2.2, 3.2.3	AT-2, AT-3, CA-5, PM-1	12.6
PPPR-19	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?	CSC 17		9.2.5	PR.AC-4, PR.PT-3	3.1.7	CA-5, PM-1	12.1, 12.5, 12.6
PPPR-20	Do you have documented, and currently implemented, internal audit processes and procedures?			12.7.1			CA-5, PM-1, PS-4, PS-5, PE-2, PE-3, PE-5, AC-6, RA-3, SA-8, CA-2, NIST SP 800-37; NIST SP 800-39; NIST SP 800-115; NIST SP 800-137	

Product Evaluation		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
PROD-01	Do you incorporate customer feedback into security feature requests?							
PROD-02	Can you provide an evaluation site to the institution for testing?				PR.DS-7			

Quality Assurance		CIS Critical Security Controls v6.1	HIPAA	ISO 27002:2013	NIST Cybersecurity Framework	NIST SP 800-171r1	NIST SP 800-53r4	PCI DSS
QLAS-01	Provide a general summary of your Quality Assurance program.	CSC 13						
QLAS-02	Do you comply with ISO 9001?	CSC 13		18.1.1				
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	CSC 13						

QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?							
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?	CSC 17						
Systems Management & Configuration		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
SYST-01	Are systems that support this service managed via a separate management network?	CSC 12		13.1.1	PR.PT-4	3.1.3	AC-4	
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	CSC 3			PR.IP-1	3.4.1, 3.4.2, 3.4.3	CM-2, CM-3, CM-6, CM-8	
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?	CSC 3		6.2.1		3.13.13		
SYST-04	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?	CSC 3		12.1.1	PR.IP-1, PR.IP-2	3.1.18, 3.7.1, 3.13.13	CM-2, CM-6, CM-3, AC-19, MA-2	
Vulnerability Scanning		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
VULN-01	Are your applications scanned externally for vulnerabilities?	CSC 4		12.6.1	DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
VULN-02	Have your applications had an external vulnerability assessment in the last year?	CSC 4		12.6.1	DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?	CSC 4			DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
VULN-04	Are your systems scanned externally for vulnerabilities?	CSC 4			DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
VULN-05	Have your systems had an external vulnerability assessment in the last year?	CSC 4			DE.CM-8		SI-2	11.2
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	CSC 4			DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2
VULN-07	Will you provide results of security scans to the Institution?	CSC 4			DE.CM-8		SI-2	11.2
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).	CSC 7, CSC 18		12.6.1	ID.RA-1, DE.CM-8, PR.IP-12	3.11.1, 3.11.2, 3.11.3, 3.14.2	SI-2	11.2, 11.3
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	CSC 20		18.2.1	DE.CM-8	3.11.1, 3.11.2, 3.11.3	SI-2	11.2, 12.8
HIPAA		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	CSC 17	§164.308(a)(5)(i)	18.1.1, 7.2.2	ID.GV-3	3.2.2	AT-3	
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	CSC 13	§164.316(b)(2)(iii)	18.1.1	ID.GV-3			
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	CSC 17	§164.308(a)(2)	18.1.1	ID.GV-3			
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	CSC 13		18.1.1	ID.GV-3			
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	CSC 19	§164.308(a)(6)(i)	16.1.1	ID.GV-3	3.6.1, 3.14.1	IR-2, IR-4, IR-5, IR-7	12.10, 10.10
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?	CSC 19	§164.308(a)(6)(ii)	16.1.2, 16.1.5, 18.1.1	ID.GV-3	3.6.2, 3.12.2	IR-6	12.8
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?	CSC 13	§164.308(a)(1)(i)		ID.GV-3			12.2
HIPA-08	Have you identified areas of risks?	CSC 4	§164.308(a)(1)(i), §164.308(a)(1)(ii)(A)		ID.GV-3			12.2

HIPA-09	Have you taken actions to mitigate the identified risks?	CSC 4	§164.308(a)(1)(ii)(B)		ID.GV-3			12.2
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	CSC 16	§164.308(a)(5)(ii)(D)	9.4.3	ID.GV-3	3.5.6	IA-4	
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?	CSC 16	§164.308(a)(5)(ii)(D)	9.4.3	ID.GV-3	3.5.9	IA-5(1)	
HIPA-12	Does your application lock-out an account after a number of failed login attempts?	CSC 16	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	9.4.3	ID.GV-3	3.1.8	AC-7	
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?	CSC 16	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	9.4.3	ID.GV-3	3.1.10, 3.1.11	AC-11, AC-11(1), AC-12	8.x
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	CSC 16	§164.308(a)(4), §164.312(d)	9.4.3	ID.GV-3	3.5.10	IA-5(1)	8.x
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	CSC 16	§164.308(a)(4), §164.312(d)		ID.GV-3			8.x
HIPA-16	Does your application provide the ability to define user access levels?	CSC 16	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)		ID.GV-3	3.1.2		8.x
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?	CSC 16, 5	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	9.1.1	ID.GV-3	3.1.2, 3.1.5		8.x
HIPA-18	Does your application support varying levels of access to records based on user ID?	CSC 16	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	9.2.3	ID.GV-3	3.1.2		8.x
HIPA-19	Is there a limit to the number of groups a user can be assigned?	CSC 16	§164.308(a)(4), §164.312(a)(1)	9.2.3	ID.GV-3			
HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	CSC 6, CSC 16	§164.308(a)(4), §164.312(a)(1)		ID.GV-3	3.3.1	AU-2, AU-6, AU-12	8.x
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?	CSC 6	§ 164.308(a)(1)(ii)(D)	12.4.1	ID.GV-3	3.3.2	AU-3	10.7
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	CSC 6	§164.312(b)	12.4.1	ID.GV-3			10.7
HIPA-23	How long does the application keep access/change logs?	CSC 6	§164.312(b)	12.4.1	ID.GV-3			10.7
HIPA-24	Can the application logs be archived?	CSC 6	§164.312(b)	12.4.1	ID.GV-3			10.7
HIPA-25	Can the application logs be saved externally?	CSC 6	§164.312(b)	12.4.1	ID.GV-3			10.7
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?	CSC 10	§164.312(a)(2)(ii)	18.1.1	ID.GV-3			10.7
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?	CSC 10	§164.308(a)(7)(i)	17.1.1	ID.GV-3	3.12.2		12.1
HIPA-28	Have the policies/plans mentioned above been tested?	CSC 10	§164.308(a)(7)(i)	17.1.3	ID.GV-3	3.6.3, 3.12.2		12.1
HIPA-29	Can you provide a HIPAA compliance attestation document?	CSC 10	§164.308(b)(2)	18.1.1	ID.GV-3			10.7
HIPA-30	Are you willing to enter into a Business Associate Agreement (BAA)?	CSC 10	§164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	18.1.1	ID.GV-3			
HIPA-31	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?	CSC 10	§164.308(a)(3)(i), §164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	18.1.1	ID.GV-3			12.8

PCI DSS		**CIS Critical Security Controls v6.1**	**HIPAA**	**ISO 27002:2013**	**NIST Cybersecurity Framework**	**NIST SP 800-171r1**	**NIST SP 800-53r4**	**PCI DSS**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?	CSC 10		18.1.1	ID.GV-3			12.8
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	CSC 10		18.1.1	ID.GV-3			12.8

PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	CSC 10		18.1.1	ID.GV-3			12.8
PCID-04	Are you classified as a service provider?				ID.GV-3			12.8
PCID-05	Are you on the list of VISA approved service providers?				ID.GV-3			12.8
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?				ID.GV-3			12.8
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	CSC 1, CSC 2			ID.GV-3			PCI Scope
PCID-08	What payment processors/gateways does the system support?	CSC 18			ID.GV-3			12.8
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	CSC 10			ID.GV-3			12.8
PCID-10	Is the application listed as an approved PA-DSS application?				ID.GV-3			12.8
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	CSC 12, CSC 13			ID.GV-3			12.8
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.	CSC 10			ID.GV-3			12.8

CIS		4
HIPAA		5
ISO		6
NIST		7
NIST SP		8
NIST SP		9
PCI DSS		10

HECVAT - Full - Analyst Report

Version 2.11

HEISC Shared Assessments Working Group

Instructions

Step 1: Select the security framework used at your institution in cell B10. **Step 2:** Convert qualitative vendor responses into quantitative values, starting at cell G37. **Step 3:** Review converted values, ensuring full population of report. **Step 4:** Move to the Summary Report tab.

Vendor Name	Vendor Name	**Product Name**	Product Name and Version Information
Vendor Contact Name	Vendor Contact Name	**Product Description**	Brief Description of the Product
Vendor Contact Title	Vendor Contact Title	**HECVAT Version**	Full
Vendor Email Address	Vendor Contact E-mail Address	**Date Prepared**	mm/dd/yyyy

Institution's Security Framework		<- Select your security framework.

Report Sections	Max_Score	Score	Score %
Documentation	105	0	0%
Application Security	375	0	0%
Authentication, Authorization, and Accounting	365	0	0%
Change Management	275	0	0%
Company	120	0	0%
Data	550	0	0%
Database	50	0	0%
Datacenter	290	0	0%
Networking	245	0	0%
Physical Security	100	0	0%
Processes	420	0	0%
Systems Management & Configuration	70	0	0%
Vulnerability Scanning	170	0	0%
Overall Score	**F**	**0**	**0%**

Qualitative Questions

ID	Question	Vendor Answer	Compliant?	
COMP-01	Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.	0		Please rate the vendor's answer
COMP-02	Describe how long your organization has conducted business in this product area.	0		Please rate the vendor's answer
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	0		Please rate the vendor's answer
APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?	0		Please rate the vendor's answer
APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-	0		Please rate the vendor's answer
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full	0		Please rate the vendor's answer
APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	0		Please rate the vendor's answer
APPL-13	Are there any OS and/or web-browser combinations that are not currently supported?	0		Please rate the vendor's answer
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and	0		Please rate the vendor's answer
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege,	0		Please rate the vendor's answer

APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).	0		Please rate the vendor's answer
AAAI-16	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events	0		Please rate the vendor's answer
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately	0		Please rate the vendor's answer
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent	0		Please rate the vendor's answer
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as	0		Please rate the vendor's answer
CHNG-07	Does the system support client customizations from one release to another?	0		Please rate the vendor's answer
DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	0		Please rate the vendor's answer
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	0		Please rate the vendor's answer
DATA-16	How long are data backups stored?	0		Please rate the vendor's answer
DCTR-07	Select the option that best describes the network segment that servers are connected to.	0		Please rate the vendor's answer
DCTR-10	List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the	0		Please rate the vendor's answer
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?	0		Please rate the vendor's answer
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	0		Please rate the vendor's answer
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.	0		Please rate the vendor's answer
FIDP-03	State and describe who has the authority to change firewall rules?	0		Please rate the vendor's answer
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?	0		Please rate the vendor's answer
QLAS-01	Provide a general summary of your Quality Assurance program.	0		Please rate the vendor's answer
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	0		Please rate the vendor's answer
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL	0		Please rate the vendor's answer
HIPAA Section Required	0		Compliant?	
HIPA-23	How long does the application keep access/change logs?	0		
Mobile App Section Required	0		Compliant?	
MAPP-01	On which mobile operating systems is your software or service supported?	0		
MAPP-02	Describe or provide a reference to the application's architecture and functionality.	0		
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?	0		
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?	0		
Third Party Section Required	0		Compliant?	
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS,	0		
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	0		
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	0		

THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better	0	
Business Continuity Section Required	0		Compliant?
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).	0	
Disaster Recovery Section Required	0		Compliant?
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	0	
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	0	
PCI DSS Section Required	0		Compliant?
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	0	
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	0	
PCID-08	What payment processors/gateways does the system support?	0	
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must	0	

Higher Education Community Vendor Assessment Tool (HECVAT) - Full - Analyst Reference

HEISC Shared Assessments Working Group

Instructions

Use this reference guide to assess vendor responses in relation to your institution's environment. The context of HECVAT questions can change, depending on implementation specifics so these recommendations and follow-up response are not exhaustive and are meant to improve assessment and report capabilities within your institution's security/risk assessment program.

Analyst tip #1: For any answer that is deem "non-compliant" by your institution, ask the vendor if there is a timeline for implementation, a sincere commitment to customer development engagement, and/or possible implementation of compensating control(s) that offsite the risks of another component.

Analyst tip #2: If a vendor's response to a follow-up inquiry is vague or seems off-point or dismissive, respond back to the vendor contact with clear expectations for a response. Responses that fail to meet expectations thereafter should be negatively assessed based on your institution's risk tolerance and the criticality of the data involved.

Analyst tip #3: The most important tip - reject a HECVAT from a vendor if; the vendor provides the institution with a insufficiently populated HECVAT; or the vendor responses are vague and/or do not answer questions directly; or significant discrepancies are found, making the HECVAT difficult to assess.

Qualifiers		Reason for Question	Follow-up Inquiries/Responses
Qualifier responses are meant to set the response requirements for a vendor and the intended use case. Since responses to these questions can make some question sections optional, vendors often answer sections partially, if they have the proper documentation. Depending on the security program maturity and risk tolerance of your institution, not all vendor responses will be relevant.			
QUAL-01	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	This qualifier determines the presence of PHI in the solution and sets the HIPAA section as required appropriately.	Reference the HIPAA section for follow-up review.
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)	The use of standalone, mobile applications is the focus of this qualifier and sets the Mobile Application section as required if in use. When a mobile application is implemented for system communication, data flows, encryption, and storage strategies on a mobile device become important.	Reference the Mobile Application section for follow-up review. Many "applications" run in a web-browser and vendors incorrectly respond due to this common word use. Ensure that responses are in the context of true mobile applications, not just web-based systems.
QUAL-03	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)	Vendors oftentimes use other vendors to supplement and/or host their infrastructures and it is important to know what, if any, institutional data is shared with fourth-parties. Responses to this qualifier set the response requirement for the Third Parties section.	Reference the Third Parties section for follow-up review.
QUAL-04	Do you have a Business Continuity Plan (BCP)?	This qualifier determines the existence of a complete, fully-populated BCP, maintained by the vendor, and sets the Business Continuity Plan section as required appropriately.	Reference the Business Continuity Plan section for follow-up review.
QUAL-05	Do you have a Disaster Recovery Plan (DRP)?	This qualifier determines the existence of a complete, fully-populated DRP, maintained by the vendor, and sets the Business Continuity Plan section as required appropriately.	Reference the Disaster Recovery Plan section for follow-up review.
QUAL-06	Will data regulated by PCI DSS reside in the vended product?	This qualifier determines the presence of PCI DSS in the solution and sets the PCI DSS section as required appropriately.	Reference the PCI DSS section for follow-up review.
QUAL-07	Is your company a consulting firm providing only consultation to the Institution?	When consultants are given access to a system containing institutional data, the "sharing" of data is not in the same context as traditional data sharing (i.e. hosting, etc.) and thus, many of the HECVAT questions do not apply. When consultants have access to a system (onsite of via remote affiliate-type accounts), the Consulting section is most relevant.	Reference the Consulting section for follow-up review.

Documentation		Reason for Question	Follow-up Inquiries/Responses
DOCU-01	Have you undergone a SSAE 18 audit?	Standard documentation, relevant to institutions requiring a vendor to undergo SSAE 16 audits.	Follow-up inquiries for SSAE 16 content will be institution/implementation specific.
DOCU-02	Have you completed the Cloud Security Alliance (CSA) self assessment or CAIQ?	Many vendors have populated a CAIQ or at least a self-assessment. Although lacking in some areas important to Higher Ed, these documents are useful for supplemental assessment.	Follow-up inquiries for CSA content will be institution/implementation specific.
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	If a vendor is STAR certified, vendor responses can theoretically be more trusted since CSA has verified their responses. Trust, but verify for yourself, as needed.	If STAR certification is important to your institution you may have specific follow-up details for documentation purposes.
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)	The details of the standard are not the focus here, it is the fact that a vendor builds their environment around a standard and that they continually evaluate and assess their security programs.	In an ideal world, a vendor will conform to an industry framework that is adopted by an institution. When this synergy does not exist, the interpretation of the vendor's responses must be interpreted in the context of the institution's environment. Follow-up inquires for industry frameworks (and levels of adoption) will be institution/implementation specific.
DOCU-05	Are you compliant with FISMA standards?	For institutions that collaborate with the United States government, FISMA compliance may be required.	Follow-up inquiries for FISMA compliance will be institution/implementation specific.
DOCU-06	Does your organization have a data privacy policy?	Managing and protecting institution data is the reason organizations perform security and risk assessments. Privacy policies outline how vendors will obtain, use, share, and protect institutional data and as such, should be robust in its language. Beware of vaguely worded privacy policies.	Inquire about any privacy language the vendor may have. It may not be ideal but there may be something available to assess or enough to have your legal counsel or policy/privacy professionals review.

Company Overview		Reason for Question	Follow-up Inquiries/Responses
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	Defining scale of company (support, resources, skillsets), General information about the organization that may be concerning.	Follow-up responses to this one are normally unique to their response. Vague answers here usually result in some footprinting of a vendor to determine their "reputation".
COMP-02	Describe how long your organization has conducted business in this product area.	We want to establish longevity of a solution and whether or not a vendor is new to the HE space.	Normally a vendor will state their overall longevity but not talk about the software/service/product under evaluation. Follow-up's includes specific questions about the origins of the software/service/product and references will be requested.

COMP-03	Do you have existing higher education customers?	Higher Ed is a unique vertical. A vendor's response to this question can help an analyst set the context for all vendor responses. Established and/or mature software/product/services are more likely to have current Higher Ed customers, and therefore understand the environment that we operate in.	A simple "Yes" without any references or supporting information should be questioned. Question the size of institutions that are using the software/product/service and the scope of their implementations.
COMP-04	Have you had a significant breach in the last 5 years?	We want transparency from the vendor and an honest answer to this question, regardless of the response, is a good step in building trust.	If a vendor says "No", it is taken at face value. If you organization is capable of conducting reconnaissance, it is encouraged. If a vendor has experienced a breach, evaluate the circumstance of the incident and what the vendor has done in response to the breach.
COMP-05	Do you have a dedicated Information Security staff or office?	Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. The size of a vendor will determine their SO size, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.	Vague responses to this question should be investigated further. Vendors without dedicated security personnel commonly have no security or security is embedded or dual-homed within operations (administrators). Ask about separation of duties, principle of least privilege, etc. - there are many ways to get additional program state information from the vendor.
COMP-06	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Understanding the development team size (and capabilities) of a vendor has a significant impact on their ability to produce and maintain code, adhering to secure coding best practices. The size of a vendor will determine their use of dedicated development teams, or lack thereof. Use the knowledge of this response when evaluating other vendor statements.	Follow-up inquiries for vendor team strategies will be unique to your institution and may depend on the underlying infrastructures needed to support a system for your specific use case.
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	For the 20% that HECVAT may not cover, this gives the vendor a chance to support their other responses. Beware when this area is populated with sales hype or other non-relevant information. Thorough documentation, supporting evidence, and/or robust responses go a long way in building trust in this assessment process.	This is a freebie to help the vendor state their "case". If a vendor does not add anything here (or it is just sales stuff), we can assume it was filled out by a sales engineer and questions will be evaluated with higher scrutiny.
Third Parties		**Reason for Question**	**Follow-up Inquiries/Responses**
THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.	Vendors oftentimes use other vendors to supplement and/or host their infrastructures and it is important to know what, if any, institutional data is shared with fourth-parties. This questions has multiple parts, therefore setting expectations that vendors provide robust responses.	Vague responses to this question should be investigated further. Vendors without documentation in relation to how they deal with other vendors is alarming.
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.	Who, what, why - that simple. If a vendor is sharing institutional data with another party, it is expected that the vendor performs their due diligence when assessing their vendors.	Vague responses to this question should be investigated further. Vendors without documentation in relation to how they deal with other vendors is alarming.
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?	Insight into legal protections for the institution and its data are the focus of this question. Understanding all stakeholder's contractual responsibilities should be clearly stated by the vendor.	Follow-up inquiries in regards to contracts will be institution/implementation specific.
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.	This is an open-ended question to allow the vendor to state the actions of their due diligence, as it pertains to safeguarding institutional data.	Vague responses to this question should be investigated further. If the vendor's effort to ensure transparency falls short, there may be a reason.
Consulting - Optional based on QUALIFIER response.		**Reason for Question**	**Follow-up Inquiries/Responses**
CONS-01	Will the consulting take place on-premises?	This question sets the stage for what the institution must do to accommodate the consultant(s). The question is important because it gives the institution the knowledge necessary to enact appropriate controls. For example, if the answer is "Yes", then access to appropriate locations can be granted, and equipment can be provisioned if needed. Whereas a "No" answer may require remote access control measures, such as the provisioning of VPN access for the consultant.	Follow-up inquiries for on-premise consulting details will be institution/implementation specific.
CONS-02	Will the consultant require access to Institution's network resources?	This question is very much about what level of network access is needed by these external consultants as it is anything else. If all that is needed is a web connection, then even simple, on-premise access to a guest network can be considered. But if it requires connectivity to a highly protected resource (for example: A database server on an isolated VLAN and only accepting traffic from a specific front end), then the consultant may need to be given access to a data center's network. Again, the purpose here is to determine what level of access is enough and what controls to put in place to secure that access.	Follow-up inquiries for on-premise consultant resource requirements will be institution/implementation specific.
CONS-03	Will the consultant require access to hardware in the Institution's data centers?	This normally is interpreted as "Does the consultant need to connect to our servers in our machine room(s)?". But, it can mean other things too. The real deeper question is, what protected resources does this consultant need to access? And why? For example: It would be unusual for an application developer to need access to a router or switch, so if that is requested, it should be questioned to see if it's reasonable.	The consultant(s) should be asked for specifics. Example: Do you need access to only the database, or also the front-end? Do you need firewall adjustments? The goal is to ask questions designed around determining what the least level of access is that will allow the consultants to complete their work.
CONS-04	Will the consultant require an account within the Institution's domain (@*.edu)?	There are occasions where a consultant needs to access a system in the same way the institution's users access it. This is most often seen in cases where code is being developed, but other scenarios exist. The answer to this question lets the institution know whether they need to alert their identity management team to provision an account for this consultant.	Ask the vendor for the reasoning for this requirement. Establish the length (time) of account use. Establish clear expectations for account use. Confirm the sponsor arrangement and ensure protections are in-place for this authorization.
CONS-05	Has the consultant received training on [sensitive, HIPAA, PCI, etc.] data handling?	Certain types of data are subject to either industry or regulatory standards. This question is designed to ensure that the contracted consultants do understand the requirements for handling those classes of data. Or, if they do not, then to give the institution time to implement another control or mitigation (for example: A training course assembled by the institution. Or contract terms designed to protect the institution by requiring that a contractor follow a specific standard).	Follow-up inquiries for consultant training will be institution/implementation specific.

CONS-06	Will any data be transferred to the consultant's possession?	This question is designed to get outright confirmation on whether your institution's data will transfer out and possibly reside, even temporarily, on the contractors' infrastructure. It is also designed to allow you to ask whether it transfers to the *company*, or to the *individual consultant*. That way, you will know what terms or controls to require (for example: 'Our institution's data can be stored and accessed on company owned equipment, but never on personally owned devices.')	Where will this be stored? Who will have access to it? How long will you retain it? Will you use secure, multi-pass erase methods to dispose of the data once the job is complete? Basically, use this as an opportunity to track what will happen to the data once it's in the contractors' hands, and also to set the expectations with the contractor on how your institution's data should be handled, stored, erased, etc.
CONS-07	Is it encrypted (at rest) while in the consultant's possession?	The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for consultant possessed data encryption at-rest will be institution/implementation specific.
CONS-08	Will the consultant need remote access to the Institution's network or systems?	Telecommuting in the IT world is common - an institution should know that proper safeguards are in place, if remote access is allowed. Vendor responses vary greatly on this so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely so there is often a gray area to interpret for this response.	Ask the vendor to summarize the reasoning behind this business process and request additional documentation that outlines the security controls implemented to safeguard institutional data.
CONS-09	Can we restrict that access based on source IP address?	Restricting access to the least number of sources is a best-practice at the focus of this question. If consultants will access institution's data from a static location, ideally the access is restricted to that static location. Based on the institution's environment, data sensitivity, and detective/preventive capabilities, the response to this question may or may not be relevant.	Follow-up inquiries for firewall rules and access control lists will be institution/implementation specific.
Application/Service Security		**Reason for Question**	**Follow-up Inquiries/Responses**
APPL-01	Do you support role-based access control (RBAC) for end-users?	Understanding access control capabilities allows an institution to estimate the type of maintenance efforts will be involved to manage a system. Depending on the users, concerns may or not be elevated. The value of this question is largely determined by the deployment strategy and use case of the software/product/service under review. This question is specific to end-users.	Ask the vendor to summarize the best practices to restrict/control the access given to the institution's end-users without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
APPL-02	Do you support role-based access control (RBAC) for system administrators?	Managing a software/product/service may rely on various professionals to administrate a system. This question is focused on how administration, and the segregation of functions, can be implemented within the system. Securing the administration portion of a system has additional implications (e.g., logging, administration, etc.) beyond that of end-users.	Ask the vendor to summarize the best practices for securing their system(s) administratively without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
APPL-03	Can employees access customer data remotely?	Telecommuting in the IT world is common - an institution should know that proper safeguards are in place, if remote access is allowed. Vendor responses vary greatly on this so confirm the context of the response if it is not clear. Many cloud services can only be managed remotely so there is often a gray area to interpret for this response.	Ask the vendor to summarize the reasoning behind this business process and request additional documentation that outlines the security controls implemented to safeguard institutional data.
APPL-04	Can you provide overall system and/or application architecture diagrams including a full description of the data communications architecture for all components of the system?	Many systems can be used a variety of ways. We want these implementation type diagrams so that we can understand the "real" use of the product.	Additional requests for documentation are made when other parts of the HECVAT are insufficient. Although helpful, many vendors do not provide supporting documentation. We try to be specific with our follow-up questions so that vendors understand we are not looking for 20-50 page whitepapers (sales documentation).
APPL-05	Does the system provide data input validation and error messages?	Input validation is a secure coding best practices so confirming its implementation is normally a high priority. Error messages (to the system and user) can be used to detect abnormal use and to better protect institutional data. Depending on the criticality of data and the flow of said data, an institution's risk tolerance will be unique to their environment.	Inquire about any planned improvements to these capabilities. Ask about their product(s) roadmap and try to understand how they prioritize security concerns in their environment.
APPL-06	Do you employ a single-tenant environment?	A vendor's response to this question can reveal a system's infrastructure quickly. Off-point responses are common here so general follow-up is often needed. Understanding how a vendor segments its customers data (or doesn't) affects various other controls, including network settings, use of encryption, access, etc.). A vendor's response here will influence potential follow-up inquiries for other HECVAT questions.	Ask the vendor to summarize why a multi-tenant (or other) environment/strategy is implemented and what compensating controls they have in place to ensure appropriate levels of confidentiality and integrity.
APPL-07	What operating system(s) is/are leveraged by the system(s)/application(s) that will have access to institution's data?	Vendor responses to this question provides clarity on environment constraints that may exist and/or influence future development, configurations, infrastructure, etc. Although the vendor response may not directly affect end-users, the risks of the underlying infrastructure is better understood.	Follow-up inquiries for operating systems leveraged by the vendor will be institution/implementation specific.
APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?	We want transparency from the vendor and an honest answer to this question, regardless of the response, is a good step in building trust.	If a vendor says "No", it is taken at face value. If you organization is capable of conducting reconnaissance, it is encouraged. If a vendor has experienced a breach, evaluate the circumstance of the incident and what the vendor has done in response to the breach.
APPL-09	Describe or provide a reference to additional software/products necessary to implement a functional system on either the backend or user-interface side of the system.	Understanding system requirements and/or dependencies (e.g., frameworks, libraries, toolkits, modules, etc.) can reveal infrastructure risks that may not be apparent by other means. In some cases, the use of trusted components may be favorable. In others, it may initiate the assessment the vendor's environment in more detail and/or expand the scope of the institution's assessment.	Follow-up inquiries concerning supplemental software/products will be institution/implementation specific.
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.	A picture is worth a thousand words. Diagrams improve transparency of the vendor's infrastructure and allows the institution to more accurately assess potential risks in a vendor's environment. Vendor's with mature infrastructures are expected to have detailed diagrams for all components of their system(s).	Refusal to share diagrams (even sanitized ones) should be met with increased concern. Ask for systems architecture diagrams (e.g., Visio, OmniGraffle, etc.). Ask for detailed data flow diagrams.
APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)	The use of n-tier architectures is best-practice, providing additional options to strength security controls. Segregating institutional data from front-end (public) systems in expected.	Follow-up inquiries for n-tier infrastructure details will be institution/implementation specific.

APPL-12	Describe or provide a reference to all web-enabled features and functionality of the system (i.e. accessed via a web-based interface).	This open-ended question allows a vendor to describe the software/product/service from the perspective of an end-user (e.g., customer). Use the vendor's response to this question to confirm the use of mobile applications or web applications. This is oftentimes misinterpreted by vendor parties [that populate the HECVAT] that do not come from a technical background.	The vendor's response to this question may reveal the need to ask additional follow-up questions to other responses.
APPL-13	Are there any OS and/or web-browser combinations that are not currently supported?	This question allows a vendor to describe situations in which their software/product/service cannot operate or be supported. The value of this question is relative, depending on the institution's operating environment.	Verify if the vendor's infrastructure is constrained by a technology or if it is a best practice that is not adopted. Ask about the vendor's future support roadmap.
APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?	User location data is a significant privacy and safety concern for individuals. Understanding a systems use and storage of user geolocation data is important.	Vague responses to this question should be met with concern. Repeat the question if first answer insufficiently - ask pointedly to ensure the vendor is not misunderstood.
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.	Managing a software/product/service may rely on various teams to administrate a system, in this question, it is security operations and systems administration. This question is focused on how system(s) administration, and the segregation of duties, are implemented in the vendor's organization, so that system administrators do not also have security responsibilities (e.g., monitoring, mitigating, reporting, etc.).	Ask the vendor to summarize the best practices for securing their system(s) administratively without the use of RBAC. Make sure to understand the administrative requirements/overhead introduced in the vendor's environment.
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)	The focus of this question is privilege creep, a situation where employees gain access privileges as they move within an organization, but privileges that they were given in previous roles are not removed. This can lead to situations were an individual has concurrent access to systems that should not be allowed.	Ask the vendor how administrator accounts are protected. Ask for documentation for their onboarding and offboarding procedures for new staff.
APPL-17	Describe or provide references explaining how tertiary services are redundant (i.e. DNS, ISP, etc.).	The focus of this question is availability. When moving to off-premise solutions, many controls and strategies implemented on-site are no longer relevant to the security of the solution.	Follow-up inquiries for tertiary services will be institution/implementation specific.
Authentication, Authorization, and Accounting		**Reason for Question**	**Follow-up Inquiries/Responses**
AAAI-01	Can you enforce password/passphrase aging requirements?	This question is primarily focused on account management capabilities that are built into a system. Although aging is not always required, a system that lacks commodity functionality may be lacking in other areas as well. Use the vendor's response to this question as a way to pivot to other questions, as needed.	The value of this question depends on your institution's policy on passwords, its use of 2FA, or any number of factors. Follow-ups for this question are unique to the institution.
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?	Many institutions have policy focused on passwords/passphrases and this question confirms the capacity of a vendor's software/product/service to comply.	Follow-up inquiries for password/passphrase complexity requirements will be institution/implementation specific.
AAAI-03	Does the system have password complexity or length limitations and/or restrictions?	Many institutions have policy focused on passwords/passphrases and this question confirms the capacity of a vendor's software/product/service to comply.	Follow-up inquiries for password/passphrase limitations and/or restrictions will be institution/implementation specific.
AAAI-04	Do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?	Account management can be a time-consuming part of an information system. Account reset capabilities, built into a system, can reduce burden on institutional support services.	Ask the vendor how end-users will be supported. Ask for training documentation or knowledgebase content. Confirm vendor and institution responsibilities in this support area (and others).
AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	If a vendor indicates that a system is standalone and cannot integrate with community standards, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?	The response to this question can reveal the use (or not) of coding best-practices. If passwords/passphrases are hard coded into systems/productions, the vendor should provide robust details supporting why this is required.	Vague responses to this question should be met with concern. Repeat the question if first answer insufficiently - ask pointedly to ensure the vendor is not misunderstood.
AAAI-07	Are user account passwords/passphrases visible in administration modules?	Vendor responses to this question provides insight into account management, authorization scope, data integrity, etc. of system administrators. Use the vendor's response to provide context for other responses.	Follow-up inquiries for administration module authorization will be institution/implementation specific.
AAAI-08	Are user account passwords/passphrases stored encrypted?	The focus of this question is confidentiality. Straight-forward question confirming the encryption of user authentication details.	Follow-up inquiries for password/passphrase encrypted storage will be institution/implementation specific.
AAAI-09	Does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	2FA/MFA, implemented correctly, strengthens the security state of a system. 2FA/MFA is commonly implemented and in many use cases, a requirement for account protection purposes.	Ask the vendor about hardware and software options, future roadmap for implementations and support, etc.
AAAI-10	Does your application support integration with other authentication and authorization systems? List which ones (such as Active Directory, Kerberos and what version) in Additional Info?	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	If a vendor indicates that a system is standalone and cannot integrate with the institution's infrastructure, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?	This is a follow-up to the questions above. Although a system may support authentication integrations, they may or may not be used on systems that store institutional data. Verify the use of authentication methods/functions in all parts of a system.	Ask for diagrams or other documentation that clearly shows what protections/systems are used and where and when they are used. The detail of inquiry will be based on the institutions risk tolerance and criticality of data.
AAAI-12	Does the system (servers/infrastructure) support external authentication services (e.g. Active Directory, LDAP) in place of local authentication?	System (technical and security) administration is complex and it is important to understand a system's capabilities to integrate with existing security and access systems. Having to maintain additional accounts increases overhead and may impact your institution's risk footprint.	Follow-up inquiries for system authentication will be unique to your institution (e.g., policy, infrastructure, etc.)
AAAI-13	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?	The purpose of this question is understand the vendor's authentication infrastructure so that additional questions can be formulated for the institution's use case.	The content of this response may or may not have value for the type of use case on the institution. Follow-up inquiries for authentication modes will be institution/implementation specific.
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?	The purpose of this question is understand the vendor's authentication infrastructure so that additional questions can be formulated for the institution's use case.	The content of this response may or may not have value for the type of use case on the institution. Follow-up inquiries for authentication modes will be institution/implementation specific.

AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?	Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is end-user logs.	If a weak response is given to this answer, it is appropriate to ask directed answers to get specific information. Ensure that questions are targeted to ensure responses will come from the appropriate party within the vendor.
AAAI-16	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.	Strong logging capabilities are vital to the proper management of a system. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk. Depending on your risk tolerance and the use case, your institution may or may not be concerned. The focus of this question is system-related logs (e.g., including but not limited to - events, state changes, control modification, etc.)	If a weak response is given to this answer, it is appropriate to ask directed answers to get specific information. Ensure that questions are targeted to ensure responses will come from the appropriate party within the vendor.
AAAI-17	Describe or provide a reference to the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how).	There are multiple components of this question - when assessing, ensure that the vendor responds to them all. Logs that are not properly managed may not be available when needed. The purpose of this question is to ensure that the vendor has a proper security mindset to ensure proper monitoring practices.	Follow-up inquiries for logging details will be institution/implementation specific.
Business Continuity Plan		**Reason for Question**	**Follow-up Inquiries/Responses**
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).	In the context of the CIA triad, this question is focused on availability and is often in need of a follow-up. Understanding the maturing of a vendor's BCP can shed light on many other aspects of a vendor's overall security state.	A vendor may have a number of BCP elements defined so the vendor's response may not be binary. Assess the components of the plan and ask about timelines, follow-up commitments, etc. If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
BCPL-02	May the Institution review your BCP and supporting documentation?	General inquiry for documentation. As BCPs may contain some sensitive data, a robust summary is appropriate in lieu of a full BCPP.	If the vendor states "No", you can ask for a summary, white paper, or blog. If unable to review the full plan, infer what you can from other BCP question responses.
BCPL-03	Is an owner assigned who is responsible for the maintenance and review of the Business Continuity Plan?	Having a BCP and maintaining/updating/testing a BCP are very different. Establishing a responsible party is fundamental to this process and this question looks to verify that within the vendor.	Follow-up inquiries for BCP responsible parties will be institution/implementation specific.
BCPL-04	Is there a defined problem/issue escalation plan in your BCP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
BCPL-05	Is there a documented communication plan in your BCP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?	It is expected that a vendor will maintain an accurate BCP to be tested at a regular interval. Any variance to this should be clearly explained. A vendor's response to this question can reveal the value that they place on testing their BCP (and possibly other aspects of their programs).	If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
BCPL-07	Has your BCP been tested in the last year?	Testing a BCP is an important action that improves the efficiency and accuracy of a vendor's continuity plans. Annual updates are generally expected.	If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
BCPL-08	Does your organization conduct training and awareness activities to validate its employees understanding of their roles and responsibilities during a crisis?	Understanding the maturity of a vendor's training and awareness program will indicate the value they place on protecting institutional data. BCP related awareness training should be prevalent, continuous, and well-documented.	If a vendor's BCP training and awareness activities are insufficient, inquire about other mandatory training, verify its scope, and confirm the training cycles.
BCPL-09	Are specific crisis management roles and responsibilities defined and documented?	As it relates to BCPs, a vendor's response will provide insight into their ability to properly response to business threats. A vendor that has not previously defined responsible parties and outlined realistic plans may not maintain the availability needed for the institution's use case or business requirement.	Follow-up inquiries for BCP roles and responsibility details will be institution/implementation specific.
BCPL-10	Does your organization have an alternative business site or a contracted Business Recovery provider?	In the event that a vendor's headquarters (primary location of operation) is no longer usable, an alternative business site may be needed to support business operations. Having an established (planned) alternative business site show maturity in a vendor's BCP.	Follow-up inquiries for alternative business site practices will be institution/implementation specific.
BCPL-11	Does your organization conduct an annual test of relocating to an alternate site for business recovery purposes?	Testing a BCP is an important action that improves the efficiency and accuracy of a vendor's continuity plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a BCP, point them to https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653
BCPL-12	Is this product a core service of your organization, and as such, the top priority during business continuity planning?	The purpose of this question is understand the vendor's order of response if affected by a unplanned business disruption. If the software/product/service being assessed is a vendor's core moneymaker, the probability that restoration of the software/product/service will be top priority.	If it is not a core service, follow-up questions should be availability focused and institution/implementation specific.
Change Management		**Reason for Question**	**Follow-up Inquiries/Responses**
CHNG-01	Do you have a documented and currently followed change management process (CMP)?	The lack of a Change Management program is indicative of immature program processes - answers to this question can provide insight into how well their responses (on the HECVAT) represent their actual environment(s).	If a weak response is given to this answer, response scrutiny should be increased. Questions about configuration management, system authority, and documentation are appropriate.
CHNG-02	Indicate all procedures that are implemented in your CMP. a.) An impact analysis of the upgrade is performed. b.) The change is appropriately authorized. c.) Changes are made first in a test environment. d.) The ability to implement the upgrades/changes in the production environment is limited to appropriate IT personnel.	This question outlines a mature Change Management process. Changes should be analyzed for impact, officially approved, tested, and performed by authorized users.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses, as needed.
CHNG-03	Will the Institution be notified of major changes to your environment that could impact the Institution's security posture?	Notification expectations should be set earlier in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
CHNG-04	Do clients have the option to not participate in or postpone an upgrade to a new release?	Unplanned and/or unexpected changes in a complex environment can introduce intolerable risks to the institution. Based on the operating environment of the institution, it may be necessary to postpone (or properly plan) the change to a system. The vendor's response should clarify their use of a "one code base" method or the ability to run multiple version concurrently.	Follow-up inquiries for software/product/service version releases will be institution/implementation specific.

CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)	Supporting multiple versions of a product is challenging. Understanding the vendor's strategy and resources will provide insight into their ability to adequately support their customers.	Follow-up inquiries for the vendor's support of concurrent versions will be institution/implementation specific.
CHNG-06	Identify the most current version of the software. Detail the percentage of live customers that are utilizing the proposed version of the software as well as each version of the software currently in use.	This question shows how easy it is for customers to upgrade from one version of the software to the next. If the software has many interdependencies, it will be difficult for customers to transition to the next version, and the software will be more difficult to support.	Follow-up inquiries for the vendor's support of concurrent versions will be institution/implementation specific.
CHNG-07	Does the system support client customizations from one release to another?	The vendor's software/product/service characteristics and the institution's use case will determine the relevancy of this question. The purpose of this question is to understand the underlying infrastructure and how it is maintained across all customers.	In cases where the software/product/service is customized for customer use cases, ensure the vendor's response covers all aspects of code migration, including backups, data conversions, local resources from the institution, etc., as it relates to code upgrades and/or version adoptions.
CHNG-08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?	Understanding the vendor's approach to approving software for production will indicate the value they place on quality assurance.	If a weak response is given to this answer, response scrutiny should be increased. Questions about software testing and reviews are appropriate.
CHNG-09	Do you have a release schedule for product updates?	Answers to this question will reveal the vendor's ability to plan in the short term. This is valuable information for customers so they can anticipate updates and potential bug fixes.	Follow-up inquiries for the vendor's product update practices will be institution/implementation specific.
CHNG-10	Do you have a technology roadmap, for the next 2 years, for enhancements and bug fixes for the product/service being assessed?	Answers to this question will reveal the vendor's ability to plan for the future of their product.	Follow-up inquiries for the vendor's technology planning practices will be institution/implementation specific.
CHNG-11	Is Institution involvement (i.e. technically or organizationally) required during product updates?	The response to this question allows the institution to understand the information technology resources required to properly maintain the vendor's system. Initial acquisition and setup is important to assess, but the long-term maintenance (and the risks that come with it), should be clearly defined. Use the response to this question to pivot to other questions and/or verify other vendor responses.	Vague responses to this question should be investigated further. Ask for additional documentation for customer responsibilities (in the context of information technology/security).
CHNG-12	Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?	Answers to this question will reveal the vendor's knowledge of their IT assets and their ability to respond to notifications about their systems and software.	Follow-up inquiries for the vendor's patching practices will be institution/implementation specific.
CHNG-13	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	New vulnerabilities are published every day and vendors have a responsibility to maintain their software(s). The fundamental nature of operation will expose some risks to the system but it is crucial that a vendor recognize their responsibilities and have a plan to implement them, when this time arrives.	Follow-up inquiries for the vendors patching practices will be institution/implementation specific.
CHNG-14	Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?	Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It's also important for troubleshooting any problems that may occur as a result of the changes.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses, as needed.
CHNG-15	Do procedures exist to provide that emergency changes are documented and authorized (including after the fact approval)?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. In the event of emergency changes, accountability and post-action review is expected.	Follow-up with a robust question set if a vendor cannot clearly state full-control of the integrity of their system(s).
Data		**Reason for Question**	**Follow-up Inquiries/Responses**
DATA-01	Do you physically and logically separate Institution's data from that of other customers?	A vendor's response to this question can reveal a system's infrastructure quickly. Off-point responses are common here so general follow-up is often needed. Understanding how a vendor segments its customers data (or doesn't) affects various other controls, including network settings, use of encryption, access, etc.). A vendor's response here will influence potential follow-up inquiries for other HECVAT questions.	Follow-up inquiries for the vendors infrastructure will be institution/implementation specific.
DATA-02	Will Institution's data be stored on any devices (database servers, file servers, SAN, NAS, …) configured with non-RFC 1918/4193 (i.e. publicly routable) IP addresses?	Systems that are directly exposed to public internet resources are at great risk than those that are not. Understanding the requirements for this configuration is important, particularly when assessing compensating controls.	Ask the vendor about their infrastructure and if there is a solution that eliminates the need for this environment.
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)	The need for encryption in transport is unique to your institution's implementation of a system. In particular, the data flow between the system and the end-users of the software/product/service.	Follow-up inquiries for data encryption between the system and end-users will be institution/implementation specific.
DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?	The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for data encryption at-rest will be institution/implementation specific.
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?	Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases if which that is not the case, be sure to understand the vendor's infrastructure and the true security of a vendor's solution.	If the vendor cannot accommodate open standards encryption requirements, direct them to NIST's Cryptographic Standards and Guidelines document at https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)	The need for encryption in transport is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control. Ensure that vendor responses cover encryption between the hosts within their system - this is the important piece that follows-up on DATA-03.□	Follow-up inquiries for data encryption within the system components (and end-users) will be institution/implementation specific.
DATA-07	List all locations (i.e. city + datacenter name) where the institution's data will be stored?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a Data Zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for data location details will be institution/implementation specific.
DATA-08	At the completion of this contract, will data be returned to the institution?	When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. This questions allows the vendor to state their general practices when a customer leaves their environment.	A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.

DATA-09	Will the institution's data be available within the system for a period of time at the completion of this contract?	When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. This questions allows the vendor to state their general practices when a customer leaves their environment.	A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.
DATA-10	Can the institution extract a full backup of data?	When cancelling a software/product/service, an institution will commonly want all institutional data that was provided to a vendor. The vendor's response should verify if the institution can extract data or if it is a manual extraction by vendor staff.	A vendor's response should be clear and concise. Be wary of vague responses to this questions and inquire about export specifics, as needed.
DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?	This question clarifies the operating model of a vendor and provides insight into the vendor-customer paradigm of a company. Knowing if the institution is of value to a vendor or if the institution's data is of value to a vendor should weigh heavily in the decision-making process.	If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
DATA-12	Are these rights retained even through a provider acquisition or bankruptcy event?	This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question - if vague, be sure to follow-up based on institutional counsel guidance.	If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
DATA-13	In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?	This question clarifies the position of the institution in the case of acquisition or bankruptcy. Expect clear responses to this question - if vague, be sure to follow-up based on institutional counsel guidance.	If a vendor's response is unsatisfactory, engage institutional counsel to appropriately address any ownership concerns.
DATA-14	Describe or provide a reference to the backup processes for the servers on which the service and/or data resides.	This is a general inquiry about backup processes. There may be some overlap with other vendor responses - this is a good place to crosscheck consistency and valid any issues that are not clear.	Follow-up inquiries for server backup process details will be institution/implementation specific.
DATA-15	Are backup copies made according to pre-defined schedules and securely stored and protected?	Restricting system updates to a standard maintenance timeframe is important for ensuring that changes to production systems do not impact operations. It's also important for troubleshooting any problems that may occur as a result of the changes. Availability is the focus of this question.	An institution's use case will drive the requirements for backup strategy. Ensure that the institution's use case and risk tolerance can be met by vendor systems.
DATA-16	How long are data backups stored?	Confidentiality of data and lifecycle media/data maintenance maturity are the focus of this question. Data retention requirements vary greatly and this question seeks clarity of vendor practices.	Follow-up inquiries for data backup (and retention) details will be institution/implementation specific.
DATA-17	Are data backups encrypted?	The need for encryption at-rest (for backups) is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for data backup encryption at-rest will be institution/implementation specific.
DATA-18	Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement), that is documented and currently implemented, for all system components? (e.g. database, system, web, etc.)	Understanding how key management is handled and the safeguards implemented by the vendor to ensure key confidentiality in all components of a system(s) can provide insight into other complex details of a vendor's infrastructure. Use vendor responses to this question as a way to pivot to other infrastructure specifics, as needed to clarify potential risks.	Follow-up with the vendor to ensure that all components of the system are consider. This includes, system-to-system, system-to-client, applications, system accounts, etc.
DATA-19	Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?	The purpose of this question is to define the scope of backup operations and the scope at which a vendor may readily recover when backup restoration is required.	Follow-up inquiries for backup content scope will be institution/implementation specific.
DATA-20	Are you performing off site backups? (i.e. digitally moved off site)	When data is moved digitally (e.g., cloud provider, vendor-owned facility, etc.) offsite, the policies and implemented procedures are important to know. The protections implemented to prevent compromise will be technical in nature and should be well-documented.	Follow-up inquiries for offsite, digital backups will be institution/implementation specific.
DATA-21	Are physical backups taken off site? (i.e. physically moved off site)	When data is moved physically (e.g. HDD, print, etc.) offsite, the policies and implemented procedures are important to know. Unencrypted data taken outside secured areas introduces unnecessary risks.	Follow-up inquiries for offsite, physical backups will be institution/implementation specific.
DATA-22	Do backups containing the institution's data ever leave the Institution's Data Zone either physically or via network routing?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?	Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
DATA-24	Does the process described in DATA-23 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?	Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.	Follow-up inquiries for DoD 5220.22-M and/or SP800-88 standards will be institution specific.
DATA-25	Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements?	Confidentiality of data and lifecycle media/data maintenance maturity are the focus of this question. Data retention requirements vary greatly and this question seeks clarity of vendor practices.	Follow-up inquiries for data retention details will be institution/implementation specific.
DATA-26	Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?	Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that media that may store institutional data is protected by well-established policy and procedure.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
DATA-27	Will you handle data in a FERPA compliant manner?	Standard documentation, relevant to institution implementations requiring FERPA compliance.	Follow-up inquiries for FERPA compliance details will be institution/implementation specific.
DATA-28	Is any institution data visible in system administration modules/tools?	Confidentiality is the focus of this question. Based on the capabilities of administrators (vendor), the institution may require additional safeguards to protect the confidentiality of data stored by/shared with a vendor (e.g., additional layer of encryption, etc.).	If institutional data is visible by [vendor] system administrators, follow-up with the vendor to understand the scope of visibility, process/procedure that administrators follow, and use cases when administrators are allowed to access (view) institutional data.
Database		**Reason for Question**	**Follow-up Inquiries/Responses**
DBAS-01	Does the database support encryption of specified data elements in storage?	Depending on the use case, full database encryption may not always be required, or ideal. The ability to encrypt specific fields (data elements) can be advantageous to a system. Performance is sometimes an issue, based on the use case, and this granular approach to encryption provides an institution more options.	Follow-up inquiries for database field encryption will be institution/implementation specific. Questions may include a timeline for this capability, performance metrics, and/or architectures that compensate for this level of encryption granularity.

DBAS-02	Do you currently use encryption in your database(s)?	Confidentiality is the focus of this question. Vendor responses to this question should be well-supported. Ensure that the vendor provides sufficient supporting documentation, as needed, to ensure that the vendor properly implements encryption in their database(s).	Dismissive or vague responses should be met with concern. Follow-up questions can include the reasoning behind not using encryption, recommendations for best-practice implementation (i.e. think diagrams), and/or any timeline for implementing this capability in the software/product/service.
Datacenter		**Reason for Question**	**Follow-up Inquiries/Responses**
DCTR-01	Does your company own the physical data center where the Institution's data will reside?	Data ownership, availability, and the use of third-parties are all somewhat connected to the response of this question.	Simple responses without supporting documentation should be me with concern. Follow-up with a vendor and request supporting documentation if the answer is in any way dismissive or off-point.
DCTR-02	Does the hosting provider have a SOC 2 Type 2 report available?	This question is relative to the response above. Understanding the ownership structure of the facility that will host institutional data is important for setting availability expectations and ensure proper contract terms are in place to protect the institution due to use of third-parties. If a vendor uses a third-party vendor to provide datacenter solutions, having that vendor's SOC 2 Type 2 provides additional insight. The ability to assess these "forth-party" vendors is based on your institution's resources. The vendor is responsible for providing this information - ensure that they handle their vendors properly.	Follow-up inquiries for additional vendor's SOC 2 Type 2 reports will be institution/implementation specific.
DCTR-03	Are the data centers staffed 24 hours a day, seven days a week (i.e., 24x7x365)?	Vendors that operate their own datacenter(s) can implement their own monitoring strategy. Use the vendor's response to this questions to verify/validate other responses related to ownership/co-location/physical security.	Follow-up inquiries for data center staffing will be institution/implementation specific.
DCTR-04	Do any of your servers reside in a co-located data center?	The purpose of this question is to confirm ownership and physical characteristics of the infrastructure responsible for storing/hosting institutional data.	Ask about sharing agreements. Ask about vetting of individuals with access to the co-location space. Ask about access controls, policies, physical environments, etc.
DCTR-05	Are your servers separated from other companies via a physical barrier, such as a cage or hardened walls?	This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.	Follow-up inquiries for system physical security will be institution/implementation specific.
DCTR-06	Does a physical barrier fully enclose the physical space preventing unauthorized physical contact with any of your devices?	This question is primarily focused on system integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.	Follow-up inquiries for system physical security will be institution/implementation specific.
DCTR-07	Select the option that best describes the network segment that servers are connected to.	Network configuration requirements vary greatly and this question give vendor's the chance to summarize their system's network infrastructure. Review the vendor's response to this question and then reassess other infrastructure components or other vendor response's that may be affected by the network infrastructure described in this response.	Standalone solutions will require follow-up questions similar to onsite consulting. SaaS solutions that are hosted in IaaS environments will have network segments and configurations appropriate for that environment. Follow-up questions will be platform/environment specific.
DCTR-08	Does this data center operate outside of the Institution's Data Zone?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for datacenter location details will be institution/implementation specific.
DCTR-09	Will any institution data leave the Institution's Data Zone?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
DCTR-10	List all datacenters and the cities, states (provinces), and countries where the Institution's data will be stored (including within the Institution's Data Zone).	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for datacenter location details will be institution/implementation specific.
DCTR-11	Are your primary and secondary data centers geographically diverse?	Geographic diversity is ideal when planning primary and secondary datacenters. The focus of this question is to determine appropriate geographic diversity to meet the availability requirements of the institution.	Inquire about future plans, backup plans for the backup plan, etc. Availability is the name of the game - focus on the needs of the institution, especially BCP and DRP elements.
DCTR-12	If outsourced or co-located, is there a contract in place to prevent data from leaving the Institution's Data Zone?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for co-location contracts will be institution/implementation specific.
DCTR-13	What Tier Level is your data center (per levels defined by the Uptime Institute)?	Standard documentation, relevant to institutions requiring a vendor to maintain a specific Uptime Institute Tier Level.	Follow-up inquiries for Uptime Institute Tier Level details will be institution/implementation specific.
DCTR-14	Is the service hosted in a high availability environment?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
DCTR-15	Is redundant power available for all datacenters where institution data will reside?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
DCTR-16	Are redundant power strategies tested?	Installing [potential] redundant power and regularly testing strategies to ensure they will work when needed are very different. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	Follow-up inquiries for redundant power testing details will be institution/implementation specific.
DCTR-17	Describe or provide a reference to the availability of cooling and fire suppression systems in all datacenters where institution data will reside.	Vendor responses will indicate the environment of the vendor's datacenter. If a vendor's "datacenter" is the spare closet at the office, additional risks are introduced to the CIA triad, and should be followed-up on appropriately.	Follow-up inquiries for cooling and fire suppression details will be institution/implementation specific.
DCTR-18	State how many Internet Service Providers (ISPs) provide connectivity to each datacenter where the institution's data will reside.	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
DCTR-19	Does every datacenter where the Institution's data will reside have multiple telephone company or network provider entrances to the facility?	In the context of the CIA triad, this question is focused on the availability of a system (or set of systems).	The weight placed on the vendor's response will be specific to the institution's use case and software/product/service requirements.
Disaster Recovery Plan		**Reason for Question**	**Follow-up Inquiries/Responses**

DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).	In the context of the CIA triad, this question is focused on availability and is often in need of a follow-up. Understanding the maturing of a vendor's DRP can shed light on many other aspects of a vendor's overall security state.	A vendor may have a number of BCP elements defined so the vendor's response may not be binary. Assess the components of the plan and ask about timelines, follow-up commitments, etc. If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-02	Is an owner assigned who is responsible for the maintenance and review of the DRP?	Having a DRP and maintaining/updating/testing a DRP are very different. Establishing a responsible party is fundamental to this process and this question looks to verify that within the vendor.	Follow-up inquiries for DRP responsible parties will be institution/implementation specific.
DRPL-03	Can the Institution review your DRP and supporting documentation?	General inquiry for documentation. As DRPs may contain some sensitive data, a robust summary is appropriate in lieu of a full DRP.	If the vendor states "No", you can ask for a summary, white paper, or blog. If unable to review the full plan, infer what you can from other DRP question responses.
DRPL-04	Are any disaster recovery locations outside the Institution's Data Zone?	Data exposure is a risk if sensitive data is in any way transported (physically or electronically) into a data zone that is not authorized by the institution. Depending on the criticality of data and institution policy, full control of data confidentiality may be highly valued.	Follow-up inquiries for data backup procedures/practices will be institution/implementation specific.
DRPL-05	Does your organization have a disaster recovery site or a contracted Disaster Recovery provider?	In the event that a vendor's headquarters (primary location of operation) is no longer usable, a recovery site may be needed to support business operations. Having an established (planned) recovery site show maturity in a vendor's DRP.	Follow-up inquiries for disaster recovery site practices will be institution/implementation specific.
DRPL-06	Does your organization conduct an annual test of relocating to this site for disaster recovery purposes?	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
DRPL-08	Is there a documented communication plan in your DRP for impacted clients?	Notification expectations should be set early in the contract/assessment process. Timelines, correspondence medium, and playbook details are all aspects to keep in mind when assessing this response.	If the vendor's response does not cover the details outlined in the reasoning, follow-up and get specific responses for each, as needed.
DRPL-09	Describe or provide a reference to how your disaster recovery plan is tested? (i.e. scope of DR tests, end-to-end testing, etc.)	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-10	Has the Disaster Recovery Plan been tested in the last year? Please provide a summary of the results in Additional Information (including actual recovery time).	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-11	Do the documented test results identify your organizations actual recovery time capabilities for technology and facilities?	The vendor's response to this question will verify other responses related to planning, testing, and metrics. Use the response to infer the maturity of the vendor's DRP efforts.	Follow-up inquiries for recovery time capabilities will be institution/implementation specific.
DRPL-12	Are all components of the DRP reviewed at least annually and updated as needed to reflect change?	Testing a DRP is an important action that improves the efficiency and accuracy of a vendor's recovery plans. Vague responses to this question should be met with concern and appropriate follow-up, based on your institutions risk tolerance.	If the vendor does not have a DRP, point them to https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164
DRPL-13	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Vendor responses to this questions need to be evaluated in the context of use case, data criticality, institutional risk tolerance, and value of the software/product/service to the institution's mission.	Follow-up inquiries for cyber-risk insurance will be institution/implementation specific.
Firewalls, IDS, IPS, and Networking		**Reason for Question**	**Follow-up Inquiries/Responses**
FIDP-01	Are you utilizing a web application firewall (WAF)?	The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.	If a vendors states that they outsource their code development and do not run a WAF, there is elevated reason for concern. Verify how code is tested, monitored, and controlled in production environments.
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?	The use case, vendor infrastructure, and types of services offered will greatly affect the need for various firewalling devices. The focus of this question is integrity, ensuring that the systems hosting institutional data are limited in need-only communications. The use of a WAF is important in systems in which a vendor has limited access to the to code infrastructure.	If a vendors states that they outsource their code development and do not run a WAF, there is elevated reason for concern. Verify how code is tested, monitored, and controlled in production environments.
FIDP-03	State and describe who has the authority to change firewall rules?	Modifications to firewall rulesets can have significant repercussions. To ensure the integrity of the ruleset, this question targets the individual (or responsible party) for changes and the reasoning behind their authority.	Ensure that a separation of duties exists in network security configurations. Pay close attention to responsibility overlap in small organizations, where staff often fill multiple roles.
FIDP-04	Do you have a documented policy for firewall change requests?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Any change to a verified, known, secure environment should be carefully evaluated by stakeholders in a structured manner.	Follow-up inquiries for firewall change requests will be institution/implementation specific.
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?	It is important to have detective capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	A security program with limited resources for event detection is not effective. Inquiries should include training for staff, reasoning behind not using IDS technologies, and how systems are monitored. Additional questions about a SIEM and other tool may be appropriate.
FIDP-06	Have you implemented an Intrusion Prevention System (network-based)?	It is important to have preventive capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	A security program with limited resources for active prevent is inefficient. Inquiries should include training for staff, reasoning behind not using IPS technologies, and how systems are actively protected and how malicious activity is stopped.

FIDP-07	Do you employ host-based intrusion detection?	It is important to have detective capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IDSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	Ask the vendor to summarize why host-based intrusion detection tools are not implemented in their environment. What compensating controls are in place to detect configuration changes and/or failures of integrity?
FIDP-08	Do you employ host-based intrusion prevention?	It is important to have preventive capabilities in an information system to protect institutional data. Somewhat expected in information systems, vendors without IPSs implemented should raise concerns. Compensating controls need future evaluation, if provided by the vendor.	Ask the vendor to summarize why host-based intrusion prevention tools are not implemented in their environment. What compensating controls are in place to detect malicious activity and to actively prevent its function.
FIDP-09	Are you employing any next-generation persistent threat (NGPT) monitoring?	This question is primarily focused on the maturity of a vendor's security program. Technologies are rapidly introduced and the toolsets needed to monitor, manage, and secure them need to keep up. Vendor responses to this question can give an institution insight into the maturity and overall state of a vendor's security.	Follow-up inquiries for NGPT monitoring will be institution/implementation specific.
FIDP-10	Do you monitor for intrusions on a 24x7x365 basis?	This question is primarily focused on system(s) integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. Depending on the use case or vendor infrastructure, this may not be relevant.	Follow-up inquiries for 24x7x365 monitoring will be institution/implementation specific.
FIDP-11	Is intrusion monitoring performed internally or by a third-party service?	This question is primarily focused on the capability of a vendor's security program. Understanding the size and skillsets of a vendor (taken from other responses) is needed to determine the appropriateness of the vendor's response to this question.	Follow-up inquiries for intrusion monitoring will be institution/implementation specific.
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?	Strong logging capabilities are vital to the proper management of a network. Implementing an immature system that lacks sufficient logging capabilities exposes an institution to great risk.	If a weak response is given to this answer, it is an indicator that a non-technical representative populated the document and response scrutiny should be increased. If a vendor does not answer appropriately, a follow-up request to have the question fully-answered is appropriate.

Mobile Applications		**Reason for Question**	**Follow-up Inquiries/Responses**
MAPP-01	On which mobile operating systems is your software or service supported?	The purpose of this question is to highlight any concerning restrictions in the software/product/service that may cause support (or other) risks when deployed.	Follow-up inquiries for mobile application compatibility will be institution/implementation specific.
MAPP-02	Describe or provide a reference to the application's architecture and functionality.	Languages, platforms, libraries, coding style - anything along these lines is what this question is after. Layers of architecture, number of systems, complexity of configuration, and commonality of hardware/software are all points of interest in this question.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that appropriate documentation exists to clearly understand the vendor's environment.
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?	Distributing application via known, moderately vetted application platform decreases the chances of malicious code distribution. Standalone deployments (non-trusted sources) should be looked at more closely.	Ask the vendor why this deployment strategy is used. Ask if it is a restriction of the app store platform or some other environment restriction.
MAPP-04	Does the application store, process, or transmit critical data?	The purpose of this question is to understand the flow of data, specifically critical data, so that the proper follow-up questions can be asked.	Ask the vendor for data flow diagrams. Communication trusts between nodes is important - ask how data is handled at the application (device end), not just the servers.
MAPP-05	Is Institution's data encrypted in transport?	The need for encryption in transport is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for data encryption in transport will be institution/implementation specific.
MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)	The need for encryption at-rest is unique to your institution's implementation of a system. In particular, system components, architectures, and data flows, all factor into the need for this control.	Follow-up inquiries for data encryption at-rest will be institution/implementation specific.
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?	This question is to set account management expectations for the institution. A system that can integrate with existing, vetted solutions, has its advantages and may have less administrative overhead. Also, adherence to standards here gives credit to other standards-oriented questions/responses.	If a vendor indicates that a system is standalone and cannot integrate with community standards, follow-up with maturity questions and ask about other commodity type functions or other system requirements your institution may have.
MAPP-08	Will any of these systems be implemented on systems hosting the Institution's data?	This is a follow-up to the questions above. Although a system may support authentication integrations, they may or may not be used on systems that store institutional data. Verify the use of authentication methods/functions in all parts of a system.	Ask for diagrams or other documentation that clearly shows what protections/systems are used and where and when they are used. The detail of inquiry will be based on the institutions risk tolerance and criticality of data.
MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
MAPP-10	Has the application been tested for vulnerabilities by a third party?	External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	If "No", inquire if there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?	External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.

Physical Security		**Reason for Question**	**Follow-up Inquiries/Responses**
PHYS-01	Does your organization have physical security controls and policies in place?	This question is primarily focused on system(s) integrity. If institutional data is stored in a system that is not physically secured from unauthorized access, the need for compensating controls is often higher. This question also encompasses office (and other) spaces used by the vendor to conduct operations.	If a weak response is given to this answer, response scrutiny should be increased. Inquire about the size of an organization, how it is physically deployed, how employees interact with each other and verify each others credibility. Any follow-up question related to physical integrity of institutional data is relevant here.

PHYS-02	Are employees allowed to take home Institution's data in any form?	In the context of the CIA triad, this question is focused on confidentiality. Printed documents, mobile device use, and remote access are all relevant to this question. A vendor's response to this question will provide insight into their overall business process. Vendor business activity that pose additional security risks should be met with increased concern.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper customer data handling activity.
PHYS-03	Are video monitoring feeds retained?	The focus of this question is the detective capabilities in the event an incident occurs in regards to institutional data.	Follow-up inquiries for video data storage will be institution/implementation specific.
PHYS-04	Are video feeds monitored by datacenter staff?	The focus of this question is the detective capabilities in the event an incident occurs in regards to institutional data.	Follow-up inquiries for video monitoring will be institution/implementation specific.
PHYS-05	Are individuals required to sign in/out for installation and removal of equipment?	Managing media (and the data within) throughout its lifecycle is crucial to the protection of institutional data. The focus of this question is confidentiality, ensuring that equipment used to store institutional data is appropriately protected.	Vague responses to this question should be investigated further. Ask for additional documentation and verify that procedure (and possibly training) exists to ensure proper media handling activity.
Policies, Procedures, and Processes		**Reason for Question**	**Follow-up Inquiries/Responses**
PPPR-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Understanding the security program size (and capabilities) of a vendor has a significant impact on their ability to respond effectively to a security incident. Vendor's will share organizational charts and additional documentation of their security program, if needed. The point of this question is to verify vendor security program maturity or confirm other findings and/or assessments.	Vague responses to this question should be investigated further. Vendors unwilling to share additional supporting documentation decrease the trust established with other responses.
PPPR-02	Do you have a documented patch management process?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed according to policy. Additionally, it is expected that devices used to access the vendor's systems are properly managed and secured.	Follow-up with a robust question set if the vendor cannot clearly state full-control of their system patching strategy. Questions about patch testing, testing environments, threat mitigation, incident remediation, etc. are appropriate.
PPPR-03	Can you accommodate encryption requirements using open standards?	Beware the use of proprietary encryption implementations. Open standard encryption, preferably mature, is often preferred. Although there may be cases if which that is not the case, be sure to understand the vendor's infrastructure and the true security of a vendor's solution.	If the vendor cannot accommodate open standards encryption requirements, direct them to NIST's Cryptographic Standards and Guidelines document at https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines
PPPR-04	Have your developers been trained in secure coding techniques?	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
PPPR-05	Was your application developed using secure coding techniques?	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?	Code analysis (prior to implementation) can decrease the number of vulnerabilities within a system. Depending on the insight a vendor has into their code, code testing should be expected. When a vendor outsources their coding efforts, the use of a web application firewall may be appropriate. In this case, reference the vendor's response to their use of a WAF.	Ask the vendor what types of tools they use in testing. And who performs the testing of the code. Are developers the ones running the security tests? If static code analysis and/or static application security testing is not conducted, point the vendor to OWASP's Testing Guide at https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
PPPR-07	Do you have software testing processes (dynamic or static) that are established and followed?	Code analysis (prior to implementation) can decrease the number of vulnerabilities within a system. Depending on the insight a vendor has into their code, code testing should be expected.	If software testing processes are not established and followed, point the vendor to OWASP's Testing Guide at https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
PPPR-08	Are information security principles designed into the product lifecycle?	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
PPPR-09	Do you have a documented systems development life cycle (SDLC)?	Mature product/software/service lifecycle management can position a vendor to sufficiently plan, implement, and manage systems that better protect institutional data.	Although withdrawn by NIST, the Security Considerations in the Systems Development Life Cycle (SP 800-64r2) document is an excellent resource to provide guidance to vendors (i.e. set expectations.) Follow-up questions to SDLC use will be institution/implementation specific.
PPPR-10	Do you have a formal incident response plan?	The ability for the vendor to respond effectively (and quickly) to a security incident is of the utmost importance. The size of a vendor's security office will determine their capabilities during a security incident but the incident response plan will oftentimes determine their effectiveness. Use the knowledge of this response when evaluating other vendor statements, particularly when discussing degraded operation states.	If the vendor does not have an incident response plan, point them to the NIST Computer Security Incident Handling Guide at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
PPPR-11	Will you comply with applicable breach notification laws?	This is a general inquiry to determine if the vendor is well-versed in applicable laws and regulations that apply in the institution's region of business operation.	If a vendor is vague in their response, follow-up with direct questions about doing business in your state/region/country and any laws that are pertinent to the institution.
PPPR-12	Will you comply with the Institution's IT policies with regards to user privacy and data protection?	This is a general inquiry to determine if the vendor has reviewed the institution's policies and are committed to complying with them.	If a vendor is vague in their response, follow-up with direct questions about the institution's policies and ensure the expectation of compliance is clear with the vendor.
PPPR-13	Is your company subject to Institution's Data Zone laws and regulations?	This is a general inquiry to determine if the vendor is well-versed in applicable laws and regulations that apply in the institution's region of business operation.	If a vendor is vague in their response, follow-up with direct questions about doing business in your state/region/country and any laws that are pertinent to the institution.
PPPR-14	Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?	The use of detective and preventive controls in the hiring process serve a valuable role in protecting institutional data. As these are often HR documented policies, a vendor should have their practices well-documented and ready for review, upon request.	Ask the vendor is background checks and/or screening are conducted in any capacity, at any time during the employment period. Ask about the precautions they take to ensure the intellectual property is secured and inquire if user data is treated in an appropriate manner.
PPPR-15	Do you require new employees to fill out agreements and review policies?	Setting the expectation of performance and increase awareness of security-related responsibilities are part of these initial-hiring documents. Oftentimes these agreements and reviews are conducted during orientation for new employees.	If a vendor's practices are not clear, inquire about training requirements for employees, especially the frequency and scope of content.

PPPR-16	Do you have documented information security policy?	A shared security [responsibility] environment is expected of vendors in today's world. Security office's cannot solely protect an institution's data. Information security, engrained in an organization, is the best case scenario for the protection of institutional data. Security awareness and practice start in a vendor's policies.	If the vendor does not have document information security policy, follow-up questions about training, company practices, awareness efforts, auditing, and system protection practices are appropriate.
PPPR-17	Do you have an information security awareness program?	Understanding the maturity of a vendor's awareness program will indicate the value they place on protecting institutional data. Security involves all parts of an organization, end-user staff included. Awareness training should be prevalent, continuous, and well-documented.	If a vendor's awareness training is not prevalent, continuous, and well-documented, it is cause for concern. Inquire about other mandatory training, verify its scope, and confirm the training cycles.
PPPR-18	Is security awareness training mandatory for all employees?	Understanding the maturity of a vendor's awareness program will indicate the value they place on protecting institutional data. Security involves all parts of an organization, end-user staff included. Awareness training should be prevalent, continuous, and well-documented.	If a vendor's awareness training is not prevalent, continuous, and well-documented, it is cause for concern. Inquire about other mandatory training, verify its scope, and confirm the training cycles.
PPPR-19	Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts?	The focus of this question is privilege creep, a situation where employees gain access privileges as they move within an organization, but privileges that they were given in previous roles are not removed. This can lead to situations were an individual has concurrent access to systems that should not be allowed.	Ask the vendor how administrator accounts are protected. Ask for documentation for their onboarding and offboarding procedures for new staff.
PPPR-20	Do you have documented, and currently implemented, internal audit processes and procedures?	The focus of this question is if they audit, how they audit, what they audit, and how it is properly documented and consistently conducted.	Follow-up inquiries for internal audit strategies will be institution/implementation specific.
Product Evaluation		**Reason for Question**	**Follow-up Inquiries/Responses**
PROD-01	Do you incorporate customer feedback into security feature requests?	Not every software/product/service will have everything an institution will need, at all times, during the lifecycle of a system. The ability to influence development efforts is a valuable position for a higher ed institution. Knowing that a vendor is listening and wants to deliver viable solutions builds trust in the implementation.	Ask how requests should be submitted, how requests are prioritized, and by whom. Ask about product roadmaps (1yr, 2yr, 5yr, depending on use case).
PROD-02	Can you provide an evaluation site to the institution for testing?	Oftentimes an institution will want to evaluate a solution before committing to purchase or deploying future functionality. Based on the use case, flexibility in product evaluation may be a requirement.	Follow-up inquiries for evaluations sites will be institution/implementation specific.
Quality Assurance		**Reason for Question**	**Follow-up Inquiries/Responses**
QLAS-01	Provide a general summary of your Quality Assurance program.	Integrity and availability are the focus of this question. The existence of a well-documented quality assurance program, with demonstrated and published metrics, may provide insight into the inner workings (mindset) of a vendor.	Institutions vary broadly on how QA is handled so any follow-up questions will be contract/institution/implementation specific.
QLAS-02	Do you comply with ISO 9001?	Standard documentation, relevant to institutions requiring a vendor to comply with ISO 9001.	Follow-up inquiries for ISO 9001 content will be institution/implementation specific.
QLAS-03	Will your company provide quality and performance metrics in relation to the scope of services and performance expectations for the services you are offering?	This question is for institutions that tie metrics and service level agreements (SLAs) or expectations (SLEs) to security reviews. The implementation strategy and use case will indicate the relevancy of this question for security/risk assessment.	Follow-up inquiries for quality and performance metrics will be contract/institution/implementation specific.
QLAS-04	Have you supplied products and/or services to the Institution (or its Campuses) in the last five years?	This is a general inquiry to determine if the vendor being assessed has done or is doing business with the institution as the time of assessment. Existing relationships, if present, can be reviewed for insights into a vendor and/or to verify other responses.	Many Higher Ed institutions are large enough that existing/former contracts exist with one entity of the college/university (e.g. School of X) but it is unknown to another. Question the vendor in-depth if you get a vague response to this question - combining licenses/purchases increases buying power.
QLAS-05	Do you have a program to keep your customers abreast of higher education and/or industry issues?	This question is used to gauge the importance of our industry (higher education) to the vendor.	This is a general information question - any follow-up will be institution/implementation specific.
Systems Management & Configuration		**Reason for Question**	**Follow-up Inquiries/Responses**
SYST-01	Are systems that support this service managed via a separate management network?	Management networks and end-user networks are often exclusive, with the intent of limiting access to elevated authorization tools. When a vendor states these networks are merged in operation, it should be met with elevated levels of concern. The focus of this question is to verify a common best practice in system management, allowing an institution to gain insight into a vendor's operating environment.	Verify if the vendor's practice is constrained by a technology or if it is just a best practice that is not adopted. In the case of constraints, ask for additional best practice implementation strategies that may compensate for the elevated risk(s).
SYST-02	Do you have an implemented system configuration management process? (e.g. secure "gold" images, etc.)	Hardware lifecycles and continuous software updates creates an always-changing landscape in information technology. The focus of this question is the integrity of a vendor's infrastructure. Mismanagement of system configurations can lead to breakdowns in layers of security.	It is expected that vendors should have robust documentation when it comes to configuration management. Vague answers to this question should be met with concern. Inquire about the device management tools in use, system lifecycles, complexity of systems, etc. and evaluate the response in the context of company capabilities (see Company Background section).
SYST-03	Are employee mobile devices managed by your company's Mobile Device Management (MDM) platform?	The focus of this question is confidentiality. Vendor employees accessing institutional data from personal, unmanaged (by vendor) devices pose a risk of loss of confidentiality.	Follow-up inquiries for mobile device management procedures/practices will be institution/implementation specific. Increased scrutiny should be placed on compensating controls, data loss prevention, access controls, auditing, etc.
SYST-04	Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)?	In the context of the CIA triad, this question is focused on system integrity, ensuring that system changes are only executed by authorized users. Additionally, it is expected that devices (for administrators, vendor staff, and affiliates)that are used to access the vendor's systems are properly managed and secured.	Follow-up with a robust question set if the vendor cannot clearly state full-control of the integrity of their system(s). Questions about administrator access on end-user devices and other maintenance and patching type questions are appropriate.
Vulnerability Scanning		**Reason for Question**	**Follow-up Inquiries/Responses**
VULN-01	Are your applications scanned externally for vulnerabilities?	External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	If "No", inquire if there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.

VULN-02	Have your applications had an external vulnerability assessment in the last year?	External verification of application security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
VULN-03	Are your applications scanned for vulnerabilities prior to new releases?	Modern technologies allow for rapid deployment of features and with them, come changes to an established code environment. The focus of this question is to verify a vendor's practice of regression testing their code and verifying that previously non-existent risks are introduced into a known, secured environment.	If "No", inquiry if there are plans to implement these processes. Ask the vendor to summarize their decision behind not scanning their applications for vulnerabilities. Prior to release.
VULN-04	Are your systems scanned externally for vulnerabilities?	External verification of system security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
VULN-05	Have your systems had an external vulnerability assessment in the last year?	External verification of system security controls in important when managing a system. Trust, but verify, is the focus of this question. HECVAT responses are taken at face-value, and verified within reason, in most cases. When a vendor can attest to, and provide externally-provided evidence supporting that attestation, it goes a long way in building trust that the vendor will appropriately protect institutional data.	If "No", inquiry is there has ever been a vulnerability scan. A short lapse in external assessment validity can be understood (if there is a planned assessment) but a significant time lapse or none whatsoever is cause for elevated levels of concern.
VULN-06	Describe or provide a reference to the tool(s) used to scan for vulnerabilities in your applications and systems.	Every infrastructure has a set of tools best suited to evaluate and protect it from vulnerability. Regardless of focus (i.e. code, hardware systems, etc.), professional, well-established tools are ideal when performing vulnerability assessment. In addition, the talent/skillset of a vulnerability assessor is also important.	Inquiries should be focused on matching tools to policy/procedures and ensuring that a vendor has the skillset/knowledge to properly scan their environments for vulnerabilities and address them adequately, when discovered.
VULN-07	Will you provide results of security scans to the Institution?	If a vendor is scanning their applications and/or systems, oftentimes an institution will want to review the report, if possible. Preferably, any finding on the reports will have a matching mitigation action.	If a vendor is hesitant to share the report, ask for a summarized version - some insight is better than none.
VULN-08	Describe or provide a reference to how you monitor for and protect against common web application security vulnerabilities (e.g. SQL injection, XSS, XSRF, etc.).	The adherence to secure coding best practices better positions a vendor to maintain the CIA triad. Use the knowledge of this response when evaluating other vendor statements, particularly those focused on development and the protection of communications. Vendors should be monitoring for and addressing these issues in their products.	If information security principles are not designed into the product lifecycle, point the vendor to OWASP's Secure Coding Practices - Quick Reference Guide at https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide Inquire about the tools a vendor uses, the interval at which systems are monitored/mitigated, and who is responsible for the process/procedure in place for this monitoring.
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?	Many Higher Ed institutions are capable of performing vulnerability assessments and/or penetration testing on their vendor's infrastructures. This question confirms the possibility of conducting these actions against the vendor's infrastructure.	Follow-up inquiries for vulnerability scanning and penetration testing will be institution/implementation specific.
HIPAA		**Reason for Question**	**Follow-up Inquiries/Responses**
HIPA-01	Do your workforce members receive regular training related to the HIPAA Privacy and Security Rules and the HITECH Act?	§164.308(a)(5)(i)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-02	Do you monitor or receive information regarding changes in HIPAA regulations?	§164.316(b)(2)(iii)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?	§164.308(a)(2)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?	Inquiry into a vendor's use of electronic health records (EHRs).	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-05	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	§164.308(a)(6)(i)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?	§164.308(a)(6)(ii)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?	§164.308(a)(1)(i)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-08	Have you identified areas of risks?	§164.308(a)(1)(i), §164.308(a)(1)(ii)(A)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-09	Have you taken actions to mitigate the identified risks?	§164.308(a)(1)(ii)(B)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-10	Does your application require user and system administrator password changes at a frequency no greater than 90 days?	§164.308(a)(5)(ii)(D)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-11	Does your application require a user to set their own password after an administrator reset or on first use of the account?	§164.308(a)(5)(ii)(D)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-12	Does your application lock-out an account after a number of failed login attempts?	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-13	Does your application automatically lock or log-out an account after a period of inactivity?	§164.308(a)(4), §164.312(a)(2)(ii), §164.312(a)(2)(iii)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?	§164.308(a)(4), §164.312(d)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-15	If the application is institution-hosted, can all service level and administrative account passwords be changed by the institution?	§164.308(a)(4), §164.312(d)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-16	Does your application provide the ability to define user access levels?	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.

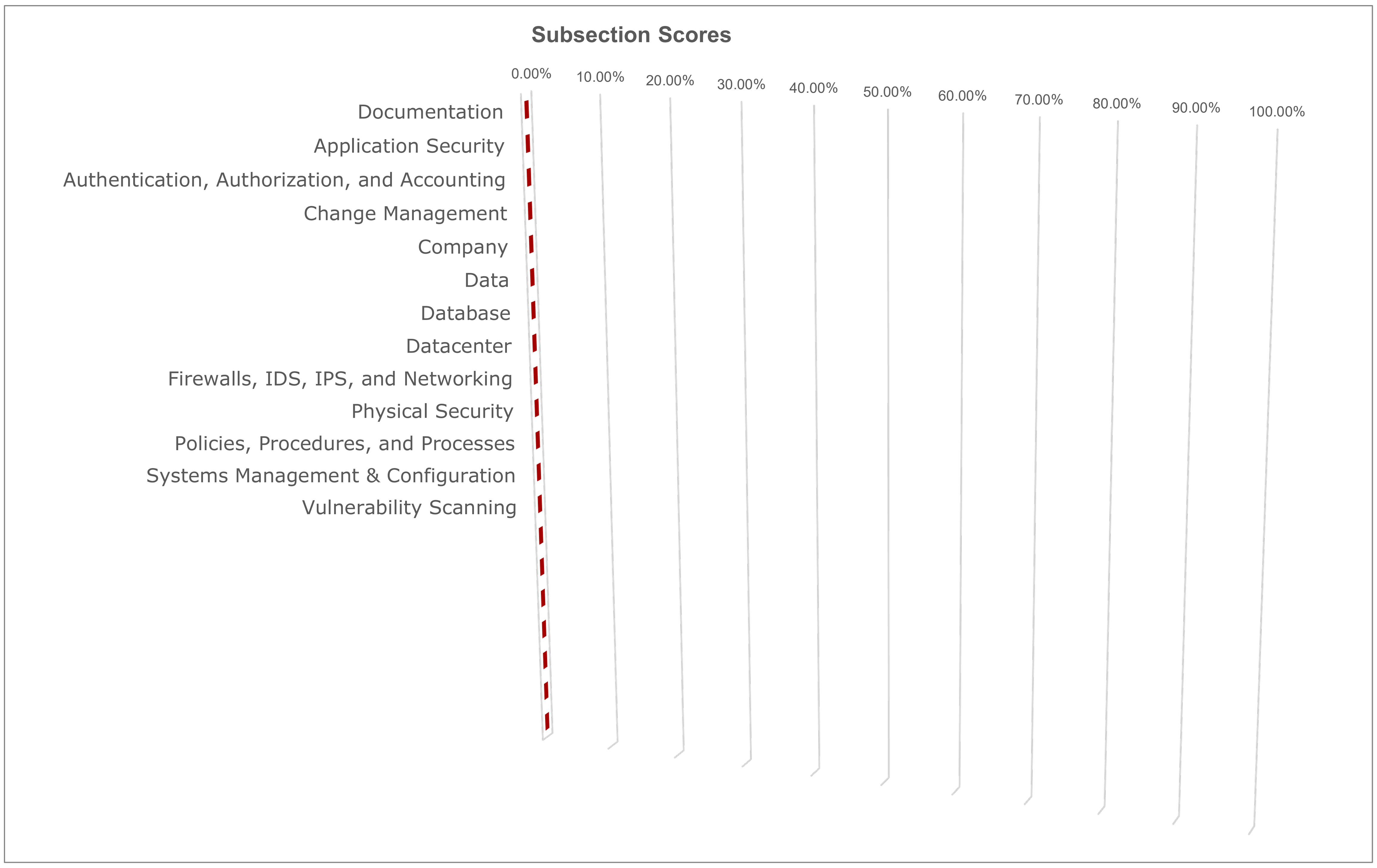
HIPA-17	Does your application support varying levels of access to administrative tasks defined individually per user?	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-18	Does your application support varying levels of access to records based on user ID?	§164.308(a)(4), §164.312(a)(1), §164.312(a)(2)(i), §164.312(d)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-19	Is there a limit to the number of groups a user can be assigned?	§164.308(a)(4), §164.312(a)(1)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-20	Do accounts used for vendor supplied remote support abide by the same authentication policies and access logging as the rest of the system?	§164.308(a)(4), §164.312(a)(1)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-21	Does the application log record access including specific user, date/time of access, and originating IP or device?	§164.308(a)(1)(ii)(D)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-22	Does the application log administrative activity, such user account access changes and password changes, including specific user, date/time of changes, and originating IP or device?	§164.312(b)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-23	How long does the application keep access/change logs?	§164.312(b)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-24	Can the application logs be archived?	§164.312(b)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-25	Can the application logs be saved externally?	§164.312(b)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-26	Does your data backup and retention policies and practices meet HIPAA requirements?	§164.312(a)(2)(ii)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-27	Do you have a disaster recovery plan and emergency mode operation plan?	§164.308(a)(7)(i)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-28	Have the policies/plans mentioned above been tested?	§164.308(a)(7)(i)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-29	Can you provide a HIPAA compliance attestation document?	§164.308(b)(2)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-30	Are you willing to enter into a Business Associate Agreement (BAA)?	§164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
HIPA-31	Have you entered into a BAA with all subcontractors who may have access to protected health information (PHI)?	§164.308(a)(3)(i), §164.308(b)(1), §164.308(b)(3), §164.314(a)(1)(i)	Follow-up inquiries for HIPAA requirements will be institution/implementation specific.
PCI DSS		**Reason for Question**	**Follow-up Inquiries/Responses**
PCID-01	Do your systems or products store, process, or transmit cardholder (payment/credit/debt card) data?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-02	Are you compliant with the Payment Card Industry Data Security Standard (PCI DSS)?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-04	Are you classified as a service provider?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-05	Are you on the list of VISA approved service providers?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-07	Describe the architecture employed by the system to verify and authorize credit card transactions.	PCI Scope	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-08	What payment processors/gateways does the system support?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-09	Can the application be installed in a PCI DSS compliant manner ?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-10	Is the application listed as an approved PA-DSS application?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-11	Does the system or products use a third party to collect, store, process, or transmit cardholder (payment/credit/debt card) data?	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.
PCID-12	Include documentation describing the systems' abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.	12.8	Follow-up inquiries for PCI DSS requirements will be institution/implementation specific.

HECVAT - Full - Summary Report

Version 2.11

Vendor	Vendor Name	**Product**	Product Name and Version Information
Description	Brief Description of the Product		

Overall Score:	
0%	F



Non-Compliant Responses

			Institution's Security Framework	
ID	**Question**	**Additional Info**	**0**	
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, ISO 27001, etc.)		#REF!	#REF!
DOCU-06	Does your organization have a data privacy policy?		#REF!	#REF!

THRD-01	Describe how you perform security assessments of third party companies with which you share data (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices that assures that the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality.		#REF!	#REF!
THRD-02	Provide a brief description for why each of these third parties will have access to institution data.		#REF!	#REF!
THRD-03	What legal agreements (i.e. contracts) do you have in place with these third parties that address liability in the event of a data breach?		#REF!	#REF!
THRD-04	Describe or provide references to your third party management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions.		#REF!	#REF!
CONS-03	Will the consultant require access to hardware in the Institution's data centers?		#REF!	#REF!
CONS-06	Will any data be transferred to the consultant's possession?		#REF!	#REF!
CONS-08	Will the consultant need remote access to the Institution's network or systems?		#REF!	#REF!
APPL-01	Do you support role-based access control (RBAC) for end-users?		#REF!	#REF!
APPL-02	Do you support role-based access control (RBAC) for system administrators?		#REF!	#REF!

APPL-06	Do you employ a single-tenant environment?		#REF!	#REF!
APPL-08	Have you or any third party you contract with that may have access or allow access to the institution's data experienced a breach?		#REF!	#REF!
APPL-10	Describe or provide a reference to the overall system and/or application architecture(s), including appropriate diagrams. Include a full description of the data communications architecture for all components of the system.		#REF!	#REF!
APPL-11	Are databases used in the system segregated from front-end systems? (e.g. web and application servers)		#REF!	#REF!
APPL-14	Can your system take advantage of mobile and/or GPS enabled mobile devices?		#REF!	#REF!
APPL-15	Describe or provide a reference to the facilities available in the system to provide separation of duties between security administration and system administration functions.		#REF!	#REF!
APPL-16	Describe or provide a reference that details how administrator access is handled (e.g. provisioning, principle of least privilege, deprovisioning, etc.)		#REF!	#REF!
AAAI-01	Can you enforce password/passphrase aging requirements?		#REF!	#REF!
AAAI-02	Can you enforce password/passphrase complexity requirements [provided by the institution]?		#REF!	#REF!

AAAI-03	Does the system have password complexity or length limitations and/or restrictions?		#REF!	#REF!
AAAI-05	Does your web-based interface support authentication, including standards-based single-sign-on? (e.g. InCommon)		#REF!	#REF!
AAAI-06	Are there any passwords/passphrases hard coded into your systems or products?		#REF!	#REF!
AAAI-07	Are user account passwords/passphrases visible in administration modules?		#REF!	#REF!
AAAI-08	Are user account passwords/passphrases stored encrypted?		#REF!	#REF!
AAAI-11	Will any external authentication or authorization system be utilized by an application with access to the institution's data?		#REF!	#REF!
AAAI-13	Does the system operate in a mixed authentication mode (i.e. external and local authentication)?		#REF!	#REF!
AAAI-14	Will any external authentication or authorization system be utilized by a system with access to institution data?		#REF!	#REF!
AAAI-15	Are audit logs available that include AT LEAST all of the following; login, logout, actions performed, and source IP address?		#REF!	#REF!

AAAI-16	Describe or provide a reference to the a) system capability to log security/authorization changes as well as user and administrator security events (i.e. physical or electronic)(e.g. login failures, access denied, changes accepted), and b) all requirements necessary to implement logging and monitoring on the system. Include c) information about SIEM/log collector usage.		#REF!	#REF!
BCPL-01	Describe or provide a reference to your Business Continuity Plan (BCP).		#REF!	#REF!
BCPL-06	Are all components of the BCP reviewed at least annually and updated as needed to reflect change?		#REF!	#REF!
BCPL-07	Has your BCP been tested in the last year?		#REF!	#REF!
CHNG-01	Do you have a documented and currently followed change management process (CMP)?		#REF!	#REF!
CHNG-05	Describe or provide a reference to your solution support strategy in relation to maintaining software currency. (i.e. how many concurrent versions are you willing to run and support?)		#REF!	#REF!
CHNG-08	Does your organization ensure through policy and procedure (that is currently implemented) that only application software verifiable as authorized, tested, and approved for production, and having met all other requirements and reviews necessary for commissioning, is placed into production?		#REF!	#REF!
DATA-01	Do you physically and logically separate Institution's data from that of other customers?		#REF!	#REF!
DATA-03	Is sensitive data encrypted in transport? (e.g. system-to-client)		#REF!	#REF!

DATA-04	Is sensitive data encrypted in storage (e.g. disk encryption, at-rest)?		#REF!	#REF!
DATA-05	Do you employ or allow any cryptographic modules that do not conform to the Federal Information Processing Standards (FIPS PUB 140-2)?		#REF!	#REF!
DATA-06	Does your system employ encryption technologies when transmitting sensitive information over TCP/IP networks (e.g., SSH, SSL/TLS, VPN)? (e.g. system-to-system and system-to-client)		#REF!	#REF!
DATA-08	At the completion of this contract, will data be returned to the institution?		#REF!	#REF!
DATA-11	Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?		#REF!	#REF!
DATA-17	Are data backups encrypted?		#REF!	#REF!
DATA-23	Do you have a media handling process, that is documented and currently implemented, including end-of-life, repurposing, and data sanitization procedures?		#REF!	#REF!
DATA-28	Is any institution data visible in system administration modules/tools?		#REF!	#REF!
DBAS-01	Does the database support encryption of specified data elements in storage?		#REF!	#REF!

DBAS-02	Do you currently use encryption in your database(s)?		#REF!	#REF!
DCTR-04	Do any of your servers reside in a co-located data center?		#REF!	#REF!
DCTR-09	Will any institution data leave the Institution's Data Zone?		#REF!	#REF!
DRPL-01	Describe or provide a reference to your Disaster Recovery Plan (DRP).		#REF!	#REF!
DRPL-07	Is there a defined problem/issue escalation plan in your DRP for impacted clients?		#REF!	#REF!
FIDP-01	Are you utilizing a web application firewall (WAF)?		#REF!	#REF!
FIDP-02	Are you utilizing a stateful packet inspection (SPI) firewall?		#REF!	#REF!
FIDP-04	Do you have a documented policy for firewall change requests?		#REF!	#REF!
FIDP-05	Have you implemented an Intrusion Detection System (network-based)?		#REF!	#REF!

FIDP-07	Do you employ host-based intrusion detection?		#REF!	#REF!
FIDP-12	Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?		#REF!	#REF!
MAPP-03	Is the application available from a trusted source (e.g., iTunes App Store, Android Market, BB World)?		#REF!	#REF!
MAPP-05	Is Institution's data encrypted in transport?		#REF!	#REF!
MAPP-06	Is Institution's data encrypted in storage? (e.g. disk encryption, at-rest)		#REF!	#REF!
MAPP-07	Does the mobile application support Kerberos, CAS, or Active Directory authentication?		#REF!	#REF!
MAPP-09	Does the application adhere to secure coding practices (e.g. OWASP, etc.)?		#REF!	#REF!
MAPP-10	Has the application been tested for vulnerabilities by a third party?		#REF!	#REF!
MAPP-11	State the party that performed the vulnerability test and the date it was conducted?		#REF!	#REF!

PHYS-02	Are employees allowed to take home Institution's data in any form?		#REF!	#REF!
PPPR-02	Do you have a documented patch management process?		#REF!	#REF!
PPPR-04	Have your developers been trained in secure coding techniques?		#REF!	#REF!
PPPR-06	Do you subject your code to static code analysis and/or static application security testing prior to release?		#REF!	#REF!
PPPR-10	Do you have a formal incident response plan?		#REF!	#REF!
PPPR-11	Will you comply with applicable breach notification laws?		#REF!	#REF!
PPPR-16	Do you have documented information security policy?		#REF!	#REF!
PPPR-17	Do you have an information security awareness program?		#REF!	#REF!
SYST-01	Are systems that support this service managed via a separate management network?		#REF!	#REF!

VULN-01	Are your applications scanned externally for vulnerabilities?		#REF!	#REF!
VULN-04	Are your systems scanned externally for vulnerabilities?		#REF!	#REF!
VULN-05	Have your systems had an external vulnerability assessment in the last year?		#REF!	#REF!
VULN-09	Will you allow the institution to perform its own security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date?		#REF!	#REF!
HIPA-03	Has your organization designated HIPAA Privacy and Security officers as required by the Rules?		#REF!	#REF!
HIPA-04	Do you comply with the requirements of the Health Information Technology for Economic and Clinical Health Act (HITECH)?		#REF!	#REF!
HIPA-06	Do you have a plan to comply with the Breach Notification requirements if there is a breach of data?		#REF!	#REF!
HIPA-07	Have you conducted a risk analysis as required under the Security Rule?		#REF!	#REF!
HIPA-14	Are passwords visible in plain text, whether when stored or entered, including service level accounts (i.e. database accounts, etc.)?		#REF!	#REF!

PCID-03	Do you have a current, executed within the past year, Attestation of Compliance (AoC) or Report on Compliance (RoC)?		#REF!	#REF!
PCID-06	Are you classified as a merchant? If so, what level (1, 2, 3, 4)?		#REF!	#REF!
PCID-09	Can the application be installed in a PCI DSS compliant manner ?		#REF!	#REF!
COMP-04	Have you had a significant breach in the last 5 years?		#REF!	#REF!
COMP-05	Do you have a dedicated Information Security staff or office?		#REF!	#REF!
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!

0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
0	0		#REF!	#REF!
			#REF!	#REF!
			#REF!	#REF!
			#REF!	#REF!
			#REF!	#REF!
			#REF!	#REF!

			#REF!	#REF!
			#REF!	#REF!
			#REF!	#REF!
			#REF!	#REF!

EDUCAUSE

Acknowledgments

The Higher Education Information Security Council Shared Assessments Working Group contributed their vision and significant talents to the conception, creation, and completion of this resource.

Members that contributed to Phase IV (2019) of this effort are:
- Jon Allen, Baylor University (working group chair)
- Matthew Buss, Internet2
- Josh Callahan, Humboldt State University
- Andrea Childress, University of Nebraska
- Tom Coffy, University of Tennessee
- Susan Coleman, REN-ISAC
- Susan Cullen, CSU Office of the Chancellor
- Michael Cyr, University of Maine System
- Debra Dandridge, Texas A&M University
- Niranjan Davray, Colgate University
- Charles Escue, Indiana University
- Carl Flynn, Baylor University
- Ruth Ginzberg, University of Wisconsin System
- Sean Hagan, Yavapai College
- Daphne Ireland, Princeton
- Brian Kelly, EDUCAUSE
- Amy Kobezak, Virginia Tech
- Nick Lewis, Internet2
- Sue McGlashan, University of Toronto
- Hector Molina, East Carolina University
- Mark Nichols, Virginia Tech
- Laura Raderman, Carnegie Mellon University
- Kyle Shachmut, Harvard University
- Bob Smith, Longwood University
- Kyle Smith, Georgia Tech
- Christian Vinten-Johansen, Penn State University
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase III (2018) of this effort are:
- Jon Allen, Baylor University
- Josh Callahan, Humboldt State University
- Susan Coleman, REN-ISAC
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Jefferson Hopkins, Purdue University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Amanda Sarratore, University of Notre Dame
- Gary Taylor, York University
- Valerie Vogel, EDUCAUSE
- Gene Willacker, Michigan State University
- David Zeichick, California State University, Chico

Members that contributed to Phase II (2017) of this effort are:
- Jon Allen, Baylor University
- Samantha Birk, IMS Global Learning Consortium
- Jeff Bohrer, IMS Global Learning Consortium
- Sarah Braun, University of Colorado - Denver
- David Cassada, University of California - Davis
- Matthew Dalton, University of Massachusetts Amherst

- Matthew Dalton, University of Massachusetts Amherst
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Todd Herring, REN-ISAC
- Kolin Hodgson, University of Notre Dame
- Tom Horton, Cornell University
- Leo Howell, North Carolina State University
- Alex Jalso, West Virginia University
- Nick Lewis, Internet2
- Wyman Miles, Cornell University
- Kim Milford, REN-ISAC
- Valerie Vogel, EDUCAUSE

Members that contributed to Phase I (2016) of this effort are:

- Jon Allen, Baylor University
- John Bruggeman, Hebrew Union College, Jewish Institute of Religion
- Charles Escue, Indiana University
- Joanna Grama, EDUCAUSE
- Karl Hassler, University of Delaware
- Todd Herring, REN-ISAC
- Nick Lewis, Internet2
- Kim Milford, REN-ISAC
- Craig Munson, Minnesota State Colleges & Universities
- Mitch Parks, University of Idaho
- Laura Raderman, Carnegie Mellon University
- Valerie Vogel, EDUCAUSE

Higher Educat

HEISC Shared Asses

Version	Date
v0.6	8/4/2016
v0.7	8/14/2016
v0.8	8/15/2016
v0.9	8/16/2016
v0.91	8/24/2016
v0.92	8/25/2016
v0.93	8/26/2016
v0.94	8/26/2016
v0.95	9/21/2016
v0.96	9/23/2016
v0.97	9/26/2016
v0.98	10/6/2016
v1.00	10/17/2016
v1.01	11/16/2016
v1.02	11/21/2016
v1.03	11/23/2016
v1.04	4/22/2017
v1.05	4/28/2017
v1.06	10/24/2017
v2.00	10/13/2018
v2.01	11/1/2018
v2.02	1/25/2019
v2.03	3/19/2019

v2.04	4/29/2019
v2.10	10/4/2019
v2.11	11/21/2019

ion Community Vendor Assessment Toolkit - Change Log

sments Working Group

Description of Change
Merged initial comments and suggestions of sub-group members.
Completed base formulas for all Guidance fields. Changed Qualifier formatting to make questions readable (and optional).
Added SOC2T2 question to datacenter section.
Added Systems and Configuration Management section, added MDM, sep. management networks, system configuration images, Internal audit processes and procedures.
Added input from WG meeting on 8/22, removed RiskMgmt section, added question ID's, and removed dup network question.
Added Introduction, Sharing Read Me, and Acknowledgements tabs and content. Also updated report specifics in Documentation.
Integrated grammatical corrections set by Karl, fixed a minor formula error in a guidance cell.
Added Instructions tab, adjusted question ID background color, updated DRP/BCP copy error.
Changed document title to HECVAT. Integrated KDH input.
Added input from NL, 36 modifications across all sections.
Updated Sharing Read Me tab with final language and options table.
Sharing Confirmation section added, updated instructions, updated Sharing Read Me tab, fixed a ton of conditional formatting issues.
Finalized for distribution.
Corrections for grammar, conditional formatting, and question clarification.
Added tertiary services narrative question (DNS, ISP, etc.).
Grammar and spelling cleanup.
Minor layout change in preparation for HECVAT-Lite split
Changed University mentions to Institution; final version before SPC 2017
Added standards crosswalk and Cloud Broker Index (CBI) information
Major revision. Visit https://www.educause.edu/hecvat for details.
Minor calculation revision in Summary Report scoring.
Cleaned up old question references, added Excel backwards compatibility through named ranges, and fixed analyst report view.
Summary Report scoring issues fixed (calculation ranges in the Questions tab, synchronized calculation steps for reporting in both the Full and Lite versions of the HECVAT); Analyst and Summary Report question

Repaired versioning issues
Updated name, converted question text on Standards Crosswalk tab to vlookups, added Analyst Reference, fixed external links
Updated SSAE 16 to 18. Fixed reference to Standards crosswalk on Summary Report.