JAMES MADISON UNIVERSITY

Request for Proposal

RFP# CMJ-1094

Parking Management System

December 17, 2020

NOTE: James Madison University will be closed for winter break from Tuesday, December 22, 2020 until Sunday, January 3, 2021

VIRGINIA ASSOCIATION OF STATE COLLEGE & UNIVERSITY PURCHASING PROFESSIONALS

VASCUPP

REQUEST FOR PROPOSAL
RFP# CMJ-1094

Issue Date: **December 17, 2020**

Title: **Parking Management System**

Issuing Agency: **Commonwealth of Virginia**
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Period of Contract: From Date of Award Through One Year (Renewable)

Sealed Proposals Will Be Received Until 2:00 PM on Tuesday, January 19, 2021 for Furnishing The Services Described Herein.

SEALED PROPOSALS MAY BE MAILED, EXPRESS MAILED, OR HAND DELIVERED DIRECTLY TO THE ISSUING AGENCY SHOWN ABOVE.

All Inquiries For Information And Clarification Should Be Directed To: Colleen Johnson, Buyer Specialist, Procurement Services, jhons9cm@jmu.edu; 540-568-3137; (Fax) 540-568-7935 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED.
In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:

_____

_____

_____

By: _____
(Signature in Ink)

Name: _____
(Please Print)

Date: _____ Title: _____

Web Address: _____ Phone: _____

Email: _____ Fax #: _____

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1_____ #2_____ #3_____ #4_____ #5_____ (please initial)

SMALL, WOMAN OR MINORITY OWNED BUSINESS:
□ YES; □ NO; *IF YES* ⇒⇒ □ SMALL; □ WOMAN; □ MINORITY ***IF MINORITY***: □ AA; □ HA; □ AsA; □ NW; □ Micro

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against an offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

REQUEST FOR PROPOSAL

RFP # CMJ-1092

TABLE OF CONTENTS

I. PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals from qualified sources to enter into a contract to provide a Parking Management System for James Madison University (JMU), an agency of the Commonwealth of Virginia. Initial contract shall be for one (1) year with an option to renew for nine (9) additional one-year periods.

II. BACKGROUND

James Madison University (JMU) is a comprehensive university in Harrisonburg, Virginia, that is part of the statewide system of public higher education in the Commonwealth. The university offers programs on the bachelor's, master's and doctoral levels with its primary emphasis on the undergraduate student. JMU's current enrollment is approximately 22,000 full and part-time students. The University employs approximately 4,000 faculty and staff.

JMU Parking Services currently manages 7 parking decks and more than 80 surface lots, providing over 14,000 parking spaces to the university's faculty, staff, students, and visitors. Each academic year the department serves more than 15,000 permit holders, facilitates parking for hundreds of campus events and issues approximately 25,000 parking citations. For the past 20 years the department has relied on T2 Systems for its parking management database software. Parking Services utilizes T2 Flex to manage parking permits, parking citations, citation appeals and campus events. Other technologies currently utilized by the department include iPads and Genetec mobile LPR for parking enforcement, Luke II pay stations and ParkMobile for metered parking, Q-Free ultrasonic sensors and signage for vehicle counting and parking guidance and Magnetic and TIBA equipment for access control. The department presently employs 17 full-time staff as well as 25 part-time student employees that assist with enforcement and special events.

III. SMALL, WOMAN-OWNED AND MINORITY PARTICIPATION

It is the policy of the Commonwealth of Virginia to contribute to the establishment, preservation, and strengthening of small businesses and businesses owned by women and minorities, and to encourage their participation in State procurement activities. The Commonwealth encourages contractors to provide for the participation of small businesses and businesses owned by women and minorities through partnerships, joint ventures, subcontracts, and other contractual opportunities. Attachment B contains information on reporting spend data with subcontractors.

IV. STATEMENT OF NEEDS

The Contractor shall have available and be able to demonstrate the use and functions of the following components and/or features of a Parking Management System. It is expected that any proposed software will already be fully developed, tested, offered publicly for sale and available immediately for installation. For this project, the University is not interested in a custom developed software. Describe in detail the manner in which each item is addressed by the system.

A. Experience, Qualifications

1. Describe prior experience and qualifications related to accomplishing the Scope of Work herein. To include details regarding:

    a. General background, experience, and qualification of vendor.

b. Provide a listing of vendor's personnel who will be directly involved with the contact, their responsibilities, and their qualification and experience.

c. Provide a list of at least three (3) current installations for the system that is being proposed. For each installation provide the following information:

i. University Name
Contact person
Address
Telephone Number
Number of students
Implementation date
Version of software (indicate if hosted on prem or SAAS)

B. Application

1. Permit Management

a. Describe ability to enter, store, access and modify data associated with each unique parking permit including permit number, date issued, expiration date, cost of permit, method of payment, customer type (faculty, staff, student, visitor, etc.), customer name, customer number, customer address, customer phone number, vehicle description, license plate number(s), etc.

b. Describe ability to manage virtual or e-permits.

c. Describe ability to assign multiple vehicles to an individual permit.

d. Describe ability to assign multiple permits to one customer.

e. Describe ability to assign one vehicle to multiple permits.

f. Describe ability to track the status of parking permits including active, lost, stolen, returned etc.

g. Describe ability to track parking permit inventory for auditing purposes.

h. Describe ability to access and track data for temporary parking permits.

i. Describe ability to create prorated parking permit fee and refund schedules.

j. Describe permit eligibility controls and eligibility waiver management capabilities.

k. Describe ability to sell permits in bulk or without associating with a particular customer (additional questions about event management in Section IV.B.8).

l. Describe any waitlist management process and capabilities.

m. Describe any capabilities for definable customer-role/eligibility based permit allocation (i.e. classifications and subclassifications [students: commuter/resident; faculty: full-time/adjunct]).

n. Describe any administrative customization of permit fields.

o. List permit table fields and properties.

2. Enforcement

a. Describe overview of system's enforcement capabilities included in the system, available as add on modules, and/or available through integrations with 3rd parties.

b. Describe availability of industry-specific handheld or commonly available iOS and Android devices.

c. Describe availability of mobile printer to pair with handheld.

d. Describe availability of maintenance programs for hardware and software.

e. Describe warrantee, repair/replacement processes, hardware service life estimates, and anticipated hardware refresh points that are anticipated across minimally the term of the proposed contract ten (10) years, or longer if hardware service life would exceed proposed term.

f. Describe capability to utilize license plate recognition technology (fixed, mobile, and handheld units).

g. Describe whether system facilitates real-time communication of citation data or requires batch process.

h. Describe ability to tire chalk vehicles or track timed parking spaces.

i. Describe ability to insert both public and private comments on citations.

3. Citation Management

a. Describe ability to enter, store, access and modify data associated with parking citations including citation number, license plate number, permit number, meter number, date, time, officer number, location, violation, vehicle description, vehicle identification number, comments, photographs, etc.

i. Specify any limitations for customization (i.e. field character limits, caps on the number of location IDs).

b. Describe ability to track the status of parking citations including payment due, payment received, paid in full, appeal pending, administrative record hold, non-sufficient funds check hold, uncollectable, etc.

i. Describe any available interface with PeopleSoft Student Administration to track/administer administrative record holds placed on students with outstanding balances.

c. Describe ability to adjust parking fines (indicate automation when relevant) including addition/removal of late fees, change violation code, assess towing charges, appeal upheld, citation void, etc.

d. Describe ability to access and process all fines associated with a specific customer simultaneously.

e. Describe ability to utilize default information from previous citation such as date, officer number, location, etc.

f. Describe internal controls (citation written, officer delete, granular settings).

g. Describe how citations are imported into the database.

h. Describe any citation appeals process and management capabilities.

i. Describe any administrative customization of citation fields.

j. List citation table fields and properties.

4. Payment Processing

a. Describe ability to access fines and fees for a particular customer including customer name, customer number, license plate number, vehicle identification number, parking permit number, parking citation number, etc.

b. Describe ability to display and process multiple fines and fees associated with a particular customer including permit fees, parking citation fines, towing charges, late penalties, etc.

c. Describe ability to process payments for citations which have not yet been entered into the system.

d. Describe any in-person, online, mobile app payment processing options.

e. Describe availability of PeopleSoft Transfer process for hard or soft transfers.

f. Describe system compatibility with third-party credit card payment processors (CashNet, Elavon, etc.).

g. Describe reconciliation processes.

5. Reporting Capabilities

    a. Describe reporting capabilities.

    b. Provide a list of all reports delivered as part of the base product including a short description of each and how reports are accessed. Include a sample of several reports for review.

    c. Describe auditing/logging functionality (complete transaction records, database objects such as permit, citation, customer modifications).

    d. Describe ability to modify existing or create custom reports.

    e. Describe ability to populate data into letter or email templates and automate batch processing of notice letters/emails.

    f. Describe what, if any, third-party software is utilized to generate and modify reports or letters.

    g. Describe ability to create reports intended to identify active permits with no payroll deduction, payroll deduction without an active permit, etc.

    h. Describe reporting output formats available.

6. Application Integration

    a. Describe any ability for integration with PeopleSoft applications (Enterprise software).

    b. Describe any ability for integration with student housing tracking software (i.e. StarRez).

    c. Define ability to interface with DMV databases to obtain vehicle owner information either internally or through a third-party vendor.

    d. Describe available integration with third-party pay-by-phone vendors.

    e. Describe available integration with third-party license plate recognition system vendors.

    f. Describe available integration with third-party multi-space metered parking vendors.

    g. Describe available integration with third-party parking guidance system vendors.

    h. Describe available integration with parking access control system vendors.

    i. Describe available integration with third-party credit card payment processors.

j. Describe compatibility with any current hardware and integrations as laid out in Section II Background Statement.

7. Event Management

   a. Describe ability to enter, store, access and modify data associated with event management including event name, description, start date and time, end date and time, event venue, parking restrictions, number of attendees, special instructions, associated permits assigned, event contact name and phone number, etc.

   b. Describe event management processing, scheduling, resource allocation, creation of standard rates per space, permit, staff resource, equipment resource, etc. that can be modified at time of sale.

   c. Describe the ways in which event information can be presented, sorted (i.e. date, venue, event name, organizer etc), and exported (Excel/Word/PDF/Other).

   d. Describe ability, if any, to track equipment loaned to another department or event organizer, such as gate permits, cones, barricades, etc. and their expected date of return.

   e. Describe ability to communicate event information to field personnel in real-time.

8. System Capabilities

   a. Describe application access management controls (internal user, role-based rights assignments with a high degree of granularity [view, edit, delete, etc.]).

   b. Describe password management.

   c. Describe customer ability to create or modify customer, vehicle, permit, appeal information via customer portal.

   d. Provide a data dictionary or schema to show the data that the system will collect/hold.

   e. Describe data protection capability, including backups.

   f. Define the system's ability to maintain historic data (i.e. past permits, citations, and transaction data).

   g. Describe any ability for the import of legacy data from the existing JMU on-premises system.

   h. Describe any ability of the system to support imagery data consisting of photographs and scanned images.

   i. Define waitlist, appeals and waivers notification methods.

j. Define webpage/app white labeling/branding/customization capability.

k. Define task scheduling capabilities.

l. Define data import/export formats supported by the system.

m. Describe system ability to enter notes in an open text field for customer, permit, citation, etc.

n. Describe system ability to print records as needed including but not limited to customer, permit, citation, appeals, etc.

o. Describe the Help system and how it can be modified.

p. Describe how the product addresses accessibility to ensure the application is accessible to people with disabilities. Describe testing for adherence to accessibility guidelines and standards. Provide documentation of the testing performed and results of that testing including the Web Accessibility and Template.

C. Application Technology

1. Provide list of all available modules and a description of each module.

2. Describe how the modules function as an integrated whole and detail any limitations in their ability to function independently from other modules.

3. Describe any transactions or functions that are not done on a real time basis and list batch jobs required for this function.

4. Describe how menus are used within the system and if menus are customizable and/or configurable. Define “customizable” and “configurable” for your application.

5. Describe the tools and expertise which university technical staff would use to support, troubleshoot, configure, or customize the application.

6. Describe customizations available with associated cost as a fixed fee or hourly rates by technician level (Section X Pricing Schedule).

7. Describe how customization impacts future updates to software.

8. Provide an architectural/technical diagram of your system.

9. Describe backup and restoration of data schedule/safeguards.

10. Describe any standard and proprietary API’s integration/connection resources, and development language and tolls that extend your toolset.

11. Describe functionality across platforms, devices, and browsers.

12. Describe your customer service support services including support contact options, standard days/hours of availability, and include specific days/hours when support is not available (e.g. holidays, etc.).

13. Describe support escalation processes.

14. Describe update/upgrade schedule.

D. Implementation, Timeline, Training

1. Describe a typical implementation timeline and project plan and include examples of previously used project plans.

2. Describe all university personnel resources required for implementation.

3. Describe any hardware required for implementation (provide pricing in Section X Pricing Schedule).

4. Describe data migration options available and any potential items not covered under implementation with rates detailed in Section X Pricing Schedule.

5. Describe training catalog. Provide detail on types of training available (i.e. included with implementation, on demand online/in person training, self-serve web trainings). Price in person (inclusive of travel costs) and remote options as relevant in Section X Pricing Schedule. Response should include differentiation between technical staff and end-user training.

6. Describe availability/approach to test and production environments.

E. Documentation

1. Provide a list of documentation provided with the product and format provided.

2. Clarify if documentation available to university users and any potential restrictions on web publication to end users.

F. Security

1. Complete and return Attachment F (Higher Education Cloud Vendor Assessment Tool) with your proposal, as per item V.A.1.b. submission instructions below.

V. PROPOSAL PREPARATION AND SUBMISSION

A. GENERAL INSTRUCTIONS

To ensure timely and adequate consideration of your proposal, offerors are to limit all contact, whether verbal or written, pertaining to this RFP to the James Madison University Procurement Office for the duration of this Proposal process. Failure to do so may jeopardize further consideration of Offeror's proposal.

1. RFP Response: In order to be considered for selection, the **Offeror shall submit a complete response to this RFP**; and shall submit to the issuing Purchasing Agency:

    a. **One (1) original** and **five (5) copies** of the entire proposal, INCLUDING ALL ATTACHMENTS. Any proprietary information should be clearly marked in accordance with 3.f. below.

    b. **One (1) electronic copy in WORD format or searchable PDF** (*CD or flash drive*) of the entire proposal, INCLUDING ALL ATTACHMENTS. **Return HECVAT Attachment F with the electronic copy as a separate Excel file.** Any proprietary information should be clearly marked in accordance with 3.f. below.

    c. Should the proposal contain **proprietary information**, provide **one (1) redacted hard copy** of the proposal and all attachments with **proprietary portions removed or blacked out**. This copy should be clearly marked "*Redacted Copy*" on the front cover. The classification of an entire proposal document, line item prices, and/or total proposal prices as proprietary or trade secrets is not acceptable. JMU shall not be responsible for the Contractor's failure to exclude proprietary information form this redacted copy.

    No other distribution of the proposal shall be made by the Offeror.

2. The version of the solicitation issued by JMU Procurement Services, as amended by an addenda, is the mandatory controlling version of the document. Any modification of, or additions to, the solicitation by the Offeror shall not modify the official version of the solicitation issued by JMU Procurement services unless accepted in writing by the University. Such modifications or additions to the solicitation by the Offeror may be cause for rejection of the proposal; however, JMU reserves the right to decide, on a case-by-case basis in its sole discretion, whether to reject such a proposal. If the modification or additions are not identified until after the award of the contract, the controlling version of the solicitation document shall still be the official state form issued by Procurement Services.

3. Proposal Preparation

    a. Proposals shall be signed by an authorized representative of the Offeror. All information requested should be submitted. Failure to submit all information requested may result in the purchasing agency requiring prompt submissions of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by the purchasing agency. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.

    b. Proposals shall be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

    c. Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, sub letter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and sub letter should be repeated at the top of the next page. The

proposal should contain a table of contents which cross references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at the appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

d. As used in this RFP, the terms "must", "shall", "should" and "may" identify the criticality of requirements. "Must" and "shall" identify requirements whose absence will have a major negative impact on the suitability of the proposed solution. Items labeled as "should" or "may" are highly desirable, although their absence will not have a large impact and would be useful, but are not necessary. Depending on the overall response to the RFP, some individual "must" and "shall" items may not be fully satisfied, but it is the intent to satisfy most, if not all, "must" and "shall" requirements. The inability of an offeror to satisfy a "must" or "shall" requirement does not automatically remove that offeror from consideration; however, it may seriously affect the overall rating of the offeror' proposal.

e. Each copy of the proposal should be bound or contained in a single volume where practical. All documentation submitted with the proposal should be contained in that single volume.

f. Ownership of all data, materials and documentation originated and prepared for the State pursuant to the RFP shall belong exclusively to the State and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by the offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act; however, the offeror must invoke the protection of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data is submitted. The written notice must specifically identify the data or materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret materials submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable and will result in rejection and return of the proposal.

4. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to James Madison University. This provides an opportunity for the Offeror to clarify or elaborate on the proposal. This is a fact-finding and explanation session only and does not include negotiation. James Madison University will schedule the time and location of these presentations. Oral presentations are an option of the University and may or may not be conducted. Therefore, proposals should be complete.

B. SPECIFIC PROPOSAL INSTRUCTIONS

Proposals should be as thorough and detailed as possible so that James Madison University may properly evaluate your capabilities to provide the required services. Offerors are required to submit the following items as a complete proposal:

1. Return RFP cover sheet and all addenda acknowledgements, if any, signed and filled out as required.

2. Plan and methodology for providing the goods/services as described in Section IV. Statement of Needs of this Request for Proposal.

3. A written narrative statement to include, but not be limited to, the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work.

4. Offeror Data Sheet, included as *Attachment A* to this RFP.

5. Small Business Subcontracting Plan, included as *Attachment B* to this RFP. Offeror shall provide a Small Business Subcontracting plan which summarizes the planned utilization of Department of Small Business and Supplier Diversity (SBSD)-certified small businesses which include businesses owned by women and minorities, when they have received Department of Small Business and Supplier Diversity (SBSD) small business certification, under the contract to be awarded as a result of this solicitation. This is a requirement for all prime contracts in excess of $100,000 unless no subcontracting opportunities exist.

6. Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: www.VASCUPP.org.

7. Proposed Cost. See Section X. Pricing Schedule of this Request for Proposal.

VI. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA

Proposals shall be evaluated by James Madison University using the following criteria:

1. Quality of products/services offered and suitability for intended purposes

2. Qualifications and experience of Offeror in providing the goods/services

3. Specific plans or methodology to be used to perform the services

4. Participation of Small, Women-Owned, & Minority (SWaM) Businesses

5. Cost

Allocation of points for evaluation criteria will be published to the eVA solicitation posting prior to the closing date and time.

B. AWARD TO MULTIPLE OFFERORS: Selection shall be made of two or more offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the evaluation factors included in the Request for Proposals, including price, if so stated in the Request for Proposals. Negotiations shall be conducted with the offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations

have been conducted with each offeror so selected, the agency shall select the offeror which, in its opinion, has made the best proposal, and shall award the contract to that offeror. The Commonwealth reserves the right to make multiple awards as a result of this solicitation. The Commonwealth may cancel this Request for Proposals or reject proposals at any time prior to an award, and is not required to furnish a statement of the reasons why a particular proposal was not deemed to be the most advantageous. Should the Commonwealth determine in writing and in its sole discretion that only one offeror is fully qualified, or that one offeror is clearly more highly qualified than the others under consideration, a contract may be negotiated and awarded to that offeror. The award document will be a contract incorporating by reference all the requirements, terms and conditions of the solicitation and the contractor's proposal as negotiated.

VII. GENERAL TERMS AND CONDITIONS

A. PURCHASING MANUAL: This solicitation is subject to the provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and Their Vendors and any revisions thereto, which are hereby incorporated into this contract in their entirety. A copy of the manual is available for review at the purchasing office. In addition, the manual may be accessed electronically at http://www.jmu.edu/procurement or a copy can be obtained by calling Procurement Services at (540) 568-3145.

B. APPLICABLE LAWS AND COURTS: This solicitation and any resulting contract shall be governed in all respects by the laws of the Commonwealth of Virginia and any litigation with respect thereto shall be brought in the courts of the Commonwealth. The Contractor shall comply with applicable federal, state and local laws and regulations.

C. ANTI-DISCRIMINATION: By submitting their proposals, offerors certify to the Commonwealth that they will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and §10 of the Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 (available for review at http://www.jmu.edu/procurement). If the award is made to a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender, sexual orientation, gender identity, or national origin and shall be subject to the same rules as other organizations that contract with public bodies to account for the use of the funds provided; however, if the faith-based organization segregates public funds into separate accounts, only the accounts and programs funded with public funds shall be subject to audit by the public body. *(§6 of the Rules Governing Procurement*).

In every contract over $10,000 the provisions in 1. and 2. below apply:

1. During the performance of this contract, the contractor agrees as follows:

    a. The contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, sexual orientation, gender identity, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the contractor. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

b. The contractor, in all solicitations or advertisements for employees placed by or on behalf of the contractor, will state that such contractor is an equal opportunity employer.

c. Notices, advertisements, and solicitations placed in accordance with federal law, rule, or regulation shall be deemed sufficient for the purpose of meeting these requirements.

2. The contractor will include the provisions of 1. above in every subcontract or purchase order over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

D. ETHICS IN PUBLIC CONTRACTING: By submitting their proposals, offerors certify that their proposals are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other offeror, supplier, manufacturer or subcontractor in connection with their proposal, and that they have not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

E. IMMIGRATION REFORM AND CONTROL ACT OF 1986: By entering into a written contract with the Commonwealth of Virginia, the Contractor certifies that the Contractor does not, and shall not during the performance of the contract for goods and services in the Commonwealth, knowingly employ an unauthorized alien as defined in the federal Immigration Reform and Control Act of 1986.

F. DEBARMENT STATUS: By submitting their proposals, offerors certify that they are not currently debarred by the Commonwealth of Virginia from submitting proposals on contracts for the type of goods and/or services covered by this solicitation, nor are they an agent of any person or entity that is currently so debarred.

G. ANTITRUST: By entering into a contract, the contractor conveys, sells, assigns, and transfers to the Commonwealth of Virginia all rights, title and interest in and to all causes of action it may now have or hereafter acquire under the antitrust laws of the United States and the Commonwealth of Virginia, relating to the particular goods or services purchased or acquired by the Commonwealth of Virginia under said contract.

H. MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS RFPs: Failure to submit a proposal on the official state form provided for that purpose may be a cause for rejection of the proposal. Modification of or additions to the General Terms and Conditions of the solicitation may be cause for rejection of the proposal; however, the Commonwealth reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a proposal.

I. CLARIFICATION OF TERMS: If any prospective offeror has questions about the specifications or other solicitation documents, the prospective offeror should contact the buyer whose name appears on the face of the solicitation no later than five working days before the due date. Any revisions to the solicitation will be made only by addendum issued by the buyer.

J. PAYMENT:

1. To Prime Contractor:

a. Invoices for items ordered, delivered and accepted shall be submitted by the contractor directly to the payment address shown on the purchase order/contract. All invoices shall show the state contract number and/or purchase order number; social security number (for individual contractors) or the federal employer identification number (for proprietorships, partnerships, and corporations).

b. Any payment terms requiring payment in less than 30 days will be regarded as requiring payment 30 days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than 30 days, however.

c. All goods or services provided under this contract or purchase order, that are to be paid for with public funds, shall be billed by the contractor at the contract price, regardless of which public agency is being billed.

d. The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.

e. Unreasonable Charges. Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, contractors should be put on notice that final payment in full is contingent on a determination of reasonableness with respect to all invoiced charges. Charges which appear to be unreasonable will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, the Commonwealth shall promptly notify the contractor, in writing, as to those charges which it considers unreasonable and the basis for the determination. A contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this section do not relieve an agency of its prompt payment obligations with respect to those charges which are not in dispute (*Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 § 53; available for review at http://www.jmu.edu/procurement*).

2. To Subcontractors:

a. A contractor awarded a contract under this solicitation is hereby obligated:

(1) To pay the subcontractor(s) within seven (7) days of the contractor's receipt of payment from the Commonwealth for the proportionate share of the payment received for work performed by the subcontractor(s) under the contract; or

(2) To notify the agency and the subcontractors, in writing, of the contractor's intention to withhold payment and the reason.

b. The contractor is obligated to pay the subcontractor(s) interest at the rate of one percent per month (unless otherwise provided under the terms of the contract) on all amounts owed by the contractor that remain unpaid seven (7) days following receipt of payment from the Commonwealth, except for amounts withheld as stated in (2) above. The date of mailing of any payment by U. S. Mail is deemed to be payment to the addressee.

These provisions apply to each sub-tier contractor performing under the primary contract. A contractor's obligation to pay an interest charge to a subcontractor may not be construed to be an obligation of the Commonwealth.

3. Each prime contractor who wins an award in which provision of a SWAM procurement plan is a condition to the award, shall deliver to the contracting agency or institution, on or before request for final payment, evidence and certification of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the SWAM procurement plan. Final payment under the contract in question may be withheld until such certification is delivered and, if necessary, confirmed by the agency or institution, or other appropriate penalties may be assessed in lieu of withholding such payment.

4. The Commonwealth of Virginia encourages contractors and subcontractors to accept electronic and credit card payments.

K. PRECENDENCE OF TERMS: Paragraphs A through J of these General Terms and Conditions and the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors, shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this solicitation, the Special Terms and Conditions shall apply.

L. QUALIFICATIONS OF OFFERORS: The Commonwealth may make such reasonable investigations as deemed proper and necessary to determine the ability of the offeror to perform the services/furnish the goods and the offeror shall furnish to the Commonwealth all such information and data for this purpose as may be requested. The Commonwealth reserves the right to inspect offeror's physical facilities prior to award to satisfy questions regarding the offeror's capabilities. The Commonwealth further reserves the right to reject any proposal if the evidence submitted by, or investigations of, such offeror fails to satisfy the Commonwealth that such offeror is properly qualified to carry out the obligations of the contract and to provide the services and/or furnish the goods contemplated therein.

M. TESTING AND INSPECTION: The Commonwealth reserves the right to conduct any test/inspection it may deem advisable to assure goods and services conform to the specifications.

N. ASSIGNMENT OF CONTRACT: A contract shall not be assignable by the contractor in whole or in part without the written consent of the Commonwealth.

O. CHANGES TO THE CONTRACT: Changes can be made to the contract in any of the following ways:

1. The parties may agree in writing to modify the scope of the contract. An increase or decrease in the price of the contract resulting from such modification shall be agreed to by the parties as a part of their written agreement to modify the scope of the contract.

2. The Purchasing Agency may order changes within the general scope of the contract at any time by written notice to the contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The contractor shall comply with the notice upon receipt. The contractor shall be compensated for any additional costs incurred as the result of such order and shall give the Purchasing Agency a credit for any savings. Said compensation shall be determined by one of the following methods:

a. By mutual agreement between the parties in writing; or

b. By agreeing upon a unit price or using a unit price set forth in the contract, if the work to be done can be expressed in units, and the contractor accounts for the number of units of work performed, subject to the Purchasing Agency's right to audit the contractor's records and/or to determine the correct number of units independently; or

c. By ordering the contractor to proceed with the work and keep a record of all costs incurred and savings realized. A markup for overhead and profit may be allowed if provided by the contract. The same markup shall be used for determining a decrease in price as the result of savings realized. The contractor shall present the Purchasing Agency with all vouchers and records of expenses incurred and savings realized. The Purchasing Agency shall have the right to audit the records of the contractor as it deems necessary to determine costs or savings. Any claim for an adjustment in price under this provision must be asserted by written notice to the Purchasing Agency within thirty (30) days from the date of receipt of the written order from the Purchasing Agency. If the parties fail to agree on an amount of adjustment, the question of an increase or decrease in the contract price or time for performance shall be resolved in accordance with the procedures for resolving disputes provided by the Disputes Clause of this contract or, if there is none, in accordance with the disputes provisions of the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors. Neither the existence of a claim nor a dispute resolution process, litigation or any other provision of this contract shall excuse the contractor from promptly complying with the changes ordered by the Purchasing Agency or with the performance of the contract generally.

P. DEFAULT: In case of failure to deliver goods or services in accordance with the contract terms and conditions, the Commonwealth, after due oral or written notice, may procure them from other sources and hold the contractor responsible for any resulting additional purchase and administrative costs. This remedy shall be in addition to any other remedies which the Commonwealth may have.

Q. INSURANCE: By signing and submitting a proposal under this solicitation, the offeror certifies that if awarded the contract, it will have the following insurance coverage at the time the contract is awarded. For construction contracts, if any subcontractors are involved, the subcontractor will have workers' compensation insurance in accordance with§ 25 of the Rules Governing Procurement – Chapter 2, Exhibit J, Attachment 1, and 65.2-800 et. Seq. of the Code of Virginia (available for review at http://www.jmu.edu/procurement) The offeror further certifies that the contractor and any subcontractors will maintain these insurance coverage during the entire term of the contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

MINIMUM INSURANCE COVERAGES AND LIMITS REQUIRED FOR MOST CONTRACTS:

1. Workers' Compensation: Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify the Commonwealth of increases in the number of employees that change their workers' compensation requirement under the Code of Virginia during the course of the contract shall be in noncompliance with the contract.

2. Employer's Liability: $100,000

3. Commercial General Liability: $1,000,000 per occurrence and $2,000,000 in the aggregate. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products and completed operations coverage. The Commonwealth of Virginia must be named as an additional insured and so endorsed on the policy.

4. Automobile Liability: $1,000,000 combined single limit. (*Required only if a motor vehicle not owned by the Commonwealth is to be used in the contract. Contractor must assure that the required coverage is maintained by the Contractor (or third party owner of such motor vehicle.*)

R. ANNOUNCEMENT OF AWARD: Upon the award or the announcement of the decision to award a contract over $100,000, as a result of this solicitation, the purchasing agency will publicly post such notice on the DGS/DPS eVA web site (www.eva.virginia.gov) for a minimum of 10 days.

S. DRUG-FREE WORKPLACE: During the performance of this contract, the contractor agrees to (i) provide a drug-free workplace for the contractor's employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the contractor's workplace and specifying the actions that will be taken against employees for violations of such prohibition; (iii) state in all solicitations or advertisements for employees placed by or on behalf of the contractor that the contractor maintains a drug-free workplace; and (iv) include the provisions of the foregoing clauses in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

For the purposes of this section, "drug-free workplace" means a site for the performance of work done in connection with a specific contract awarded to a contractor, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance or marijuana during the performance of the contract.

T. NONDISCRIMINATION OF CONTRACTORS: An offeror, or contractor shall not be discriminated against in the solicitation or award of this contract because of race, religion, color, sex, sexual orientation, gender identity, national origin, age, disability, faith-based organizational status, any other basis prohibited by state law relating to discrimination in employment or because the offeror employs ex-offenders unless the state agency, department or institution has made a written determination that employing ex-offenders on the specific contract is not in its best interest. If the award of this contract is made to a faith-based organization and an individual, who applies for or receives goods, services, or disbursements provided pursuant to this contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

U. eVA BUSINESS TO GOVERNMENT VENDOR REGISTRATION, CONTRACTS, AND ORDERS: The eVA Internet electronic procurement solution, website portal www.eVA.virginia.gov, streamlines and automates government purchasing activities in the Commonwealth. The eVA portal is the gateway for vendors to conduct business with state agencies and public bodies. All vendors desiring to provide goods and/or services to the

Commonwealth shall participate in the eVA Internet eprocurement solution by completing the free eVA Vendor Registration. All offerors must register in eVA and pay the Vendor Transaction Fees specified below; failure to register will result in the proposal being rejected. Vendor transaction fees are determined by the date the original purchase order is issued and the current fees are as follows:

Vendor transaction fees are determined by the date the original purchase order is issued and the current fees are as follows:

1. For orders issued July 1, 2014 and after, the Vendor Transaction Fee is:

   a. Department of Small Business and Supplier Diversity (SBSD) certified Small Businesses: 1% capped at $500 per order.

   b. Businesses that are not Department of Small Business and Supplier Diversity (SBSD) certified Small Businesses: 1% capped at $1,500 per order.

2. For orders issued prior to July 1, 2014 the vendor transaction fees can be found at www.eVA.virginia.gov.

3. The specified vendor transaction fee will be invoiced by the Commonwealth of Virginia Department of General Services approximately 60 days after the corresponding purchase order is issued and payable 30 days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

V. AVAILABILITY OF FUNDS: It is understood and agreed between the parties herein that the Commonwealth of Virginia shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

W. PRICING CURRENCY: Unless stated otherwise in the solicitation, offerors shall state offered prices in U.S. dollars.

X. E-VERIFY REQUIREMENT OF ANY CONTRACTOR: Any employer with more than an average of 50 employees for the previous 12 months entering into a contract in excess of $50,000 with James Madison University to perform work or provide services pursuant to such contract shall register and participate in the E-Verify program to verify information and work authorization of its newly hired employees performing work pursuant to any awarded contract.

Y. CIVILITY IN STATE WORKPLACES: The contractor shall take all reasonable steps to ensure that no individual, while performing work on behalf of the contractor or any subcontractor in connection with this agreement (each, a "Contract Worker"), shall engage in 1) harassment (including sexual harassment), bullying, cyber-bullying, or threatening or violent conduct, or 2) discriminatory behavior on the basis of race, sex, color, national origin, religious belief, sexual orientation, gender identity or expression, age, political affiliation, veteran status, or disability.

The contractor shall provide each Contract Worker with a copy of this Section and will require Contract Workers to participate in training on civility in the State workplace. Upon request, the contractor shall provide documentation that each Contract Worker has received such training.

For purposes of this Section, "State workplace" includes any location, permanent or temporary, where a Commonwealth employee performs any work-related duty or is representing his or her

agency, as well as surrounding perimeters, parking lots, outside meeting locations, and means of travel to and from these locations. Communications are deemed to occur in a State workplace if the Contract Worker reasonably should know that the phone number, email, or other method of communication is associated with a State workplace or is associated with a person who is a State employee.

The Commonwealth of Virginia may require, at its sole discretion, the removal and replacement of any Contract Worker who the Commonwealth reasonably believes to have violated this Section.

This Section creates obligations solely on the part of the contractor. Employees or other third parties may benefit incidentally from this Section and from training materials or other communications distributed on this topic , but the Parties to this agreement intend this Section to be enforceable solely by the Commonwealth and not by employees or other third parties.

Z. TRANSPORTATION AND PACKAGING: By submitting their proposals, all Offerors certify and warrant that the price offered for FOB destination includes only the actual freight rate costs at the lowest and best rate and is based upon the actual weight of the goods to be shipped. Except as otherwise specified herein, standard commercial packaging, packing and shipping containers shall be used. All shipping containers shall be legibly marked or labeled on the outside with purchase order number, commodity description, and quantity.

VIII. SPECIAL TERMS AND CONDITIONS

A. AUDIT: The Contractor hereby agrees to retain all books, records, systems, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. The Commonwealth of Virginia, its authorized agents, and/or State auditors shall have full access to and the right to examine any of said materials during said period.

B. CANCELLATION OF CONTRACT: James Madison University reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

C. IDENTIFICATION OF PROPOSAL ENVELOPE: The signed proposal should be returned in a separate envelope or package, sealed and identified as follows:

From: _____

Name of Offeror Due Date Time

_____

Street or Box No. RFP #

_____

City, State, Zip Code RFP Title

Name of Purchasing Officer: _____

The envelope should be addressed as directed on the title page of the solicitation.

The Offeror takes the risk that if the envelope is not marked as described above, it may be inadvertently opened and the information compromised, which may cause the proposal to be disqualified. Proposals may be hand-delivered to the designated location in the office issuing the solicitation. No other correspondence or other proposals should be placed in the envelope.

D. LATE PROPOSALS: To be considered for selection, proposals must be received by the issuing office by the designated date and hour. The official time used in the receipt of proposals is that time on the automatic time stamp machine in the issuing office. Proposals received in the issuing office after the date and hour designated are automatically non responsive and will not be considered. The University is not responsible for delays in the delivery of mail by the U.S. Postal Service, private couriers, or the intra university mail system. It is the sole responsibility of the Offeror to ensure that its proposal reaches the issuing office by the designated date and hour.

E. UNDERSTANDING OF REQUIREMENTS: It is the responsibility of each offeror to inquire about and clarify any requirements of this solicitation that is not understood. The University will not be bound by oral explanations as to the meaning of specifications or language contained in this solicitation. Therefore, all inquiries deemed to be substantive in nature must be in writing and submitted to the responsible buyer in the Procurement Services Office. Offerors must ensure that written inquiries reach the buyer at least five (5) days prior to the time set for receipt of offerors proposals. A copy of all queries and the respective response will be provided in the form of an addendum to all offerors who have indicated an interest in responding to this solicitation. Your signature on your Offer certifies that you fully understand all facets of this solicitation. These questions may be sent by Fax to 540/568-7935.

F. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for a period of nine (9) successive one year periods under the terms and conditions of the original contract except as stated in 1. and 2. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew shall be given approximately 90 days prior to the expiration date of each contract period.

1. If the Commonwealth elects to exercise the option to renew the contract for an additional one-year period, the contract price(s) for the additional one year shall not exceed the contract price(s) of the original contract increased/decreased by no more than the percentage increase/decrease of the other services category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

2. If during any subsequent renewal periods, the Commonwealth elects to exercise the option to renew the contract, the contract price(s) for the subsequent renewal period shall not exceed the contract price(s) of the previous renewal period increased/decreased by more than the percentage increase/decrease of the other services category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

G. SUBMISSION OF INVOICES: All invoices shall be submitted within sixty days of contract term expiration for the initial contract period as well as for each subsequent contract renewal period. Any invoices submitted after the sixty day period will not be processed for payment.

H. OPERATING VEHICLES ON JAMES MADISON UNIVERSITY CAMPUS: Operating vehicles on sidewalks, plazas, and areas heavily used by pedestrians is prohibited. In the unlikely event a driver should find it necessary to drive on James Madison University sidewalks, plazas, and areas heavily used by pedestrians, the driver must yield to pedestrians.

For a complete list of parking regulations, please go to www.jmu.edu/parking; or to acquire a service representative parking permit, contact Parking Services at 540.568.3300. The safety of our students, faculty and staff is of paramount importance to us. Accordingly, violators may be charged.

I. PRIME CONTRACTOR RESPONSIBILITIES: The contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime contractor. The contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

J. SUBCONTRACTS**:** No portion of the work shall be subcontracted without prior written consent of the purchasing agency. In the event that the contractor desires to subcontract some part of the work specified herein, the contractor shall furnish the purchasing agency the names, qualifications and experience of their proposed subcontractors. The contractor shall, however, remain fully liable and responsible for the work to be done by its subcontractor(s) and shall assure compliance with all requirements of the contract.

K. COOPERATIVE PURCHASING / USE OF AGREEMENT BY THIRD PARTIES: It is the intent of this solicitation and resulting contract(s) to allow for cooperative procurement. Accordingly, any public body, (to include government/state agencies, political subdivisions, etc.), cooperative purchasing organizations, public or private health or educational institutions or any University related foundation and affiliated corporations may access any resulting contract if authorized by the Contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) will be extended to the entities indicated above to purchase goods and services in accordance with contract terms. As a separate contractual relationship, the participating entity will place its own orders directly with the Contractor(s) and shall fully and independently administer its use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the University. No modification of this contract or execution of a separate agreement is required to participate; however, the participating entity and the Contractor may modify the terms and conditions of this contract to accommodate specific governing laws, regulations, policies, and business goals required by the participating entity. Any such modification will apply solely between the participating entity and the Contractor.

The Contractor will notify the University in writing of any such entities accessing this contract. The Contractor will provide semi-annual usage reports for all entities accessing the contract. The University shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that the University is not responsible for the acts or omissions of any entity and will not be considered in default of the contract no matter the circumstances.

Use of this contract(s) does not preclude any participating entity from using other contracts or competitive processes as needed.

L. SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:

1. It is the goal of the Commonwealth that 42% of its purchases are made from small businesses. This includes discretionary spending in prime contracts and subcontracts. All potential offerors are required to submit a Small Business Subcontracting Plan. Unless the

offeror is registered as a Department of Small Business and Supplier Diversity (SBSD)-certified small business and where it is practicable for any portion of the awarded contract to be subcontracted to other suppliers, the contractor is encouraged to offer such subcontracting opportunities to SBSD-certified small businesses. This shall not exclude SBSD-certified women-owned and minority-owned businesses when they have received SBSD small business certification. No offeror or subcontractor shall be considered a Small Business, a Women-Owned Business or a Minority-Owned Business unless certified as such by the Department of Small Business and Supplier Diversity (SBSD) by the due date for receipt of proposals. If small business subcontractors are used, the prime contractor agrees to report the use of small business subcontractors by providing the purchasing office at a minimum the following information: name of small business with the SBSD certification number or FEIN, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product/service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807.**

2. Each prime contractor who wins an award in which provision of a small business subcontracting plan is a condition of the award, shall deliver to the contracting agency or institution with every request for payment, evidence of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the small business subcontracting plan. **This information shall be submitted to: JMU Office of Procurement Services, SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807**. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm with the Department of Small Business and Supplier Diversity (SBSD) certification number or FEIN number, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product or service provided. Payment(s) may be withheld until compliance with the plan is received and confirmed by the agency or institution. The agency or institution reserves the right to pursue other appropriate remedies to include, but not be limited to, termination for default.

3. Each prime contractor who wins an award valued over $200,000 shall deliver to the contracting agency or institution with every request for payment, information on use of subcontractors that are not Department of Small Business and Supplier Diversity (SBSD)-certified small businesses. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm, phone number, FEIN number, total dollar amount subcontracted, and type of product or service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807**.

M. AUTHORIZATION TO CONDUCT BUSINESS IN THE COMMONWEALTH: A contractor organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership or registered as a registered limited liability partnership shall be authorized to transact business in the Commonwealth as a domestic or foreign business entity if so required by Title 13.1 or Title 50 of the Code of Virginia or as otherwise required by law. Any business entity described above that enters into a contract with a public body shall not allow its existence to lapse or its certificate of authority or registration to transact business in the Commonwealth, if so required under Title 13.1 or Title 50, to be revoked or cancelled at any time during the term of the contract. A public body may void any contract with a business entity if the business entity fails to remain in compliance with the provisions of this section.

N. PUBLIC POSTING OF COOPERATIVE CONTRACTS: James Madison University maintains a web-based contracts database with a public gateway access. Any resulting cooperative contract/s to this solicitation will be posted to the publicly accessible website. Contents identified as proprietary information will not be made public.

O. CRIMINAL BACKGROUND CHECKS OF PERSONNEL ASSIGNED BY CONTRACTOR TO PERFORM WORK ON JMU PROPERTY: The Contractor shall obtain criminal background checks on all of their contracted employees who will be assigned to perform services on James Madison University property. The results of the background checks will be directed solely to the Contractor. The Contractor bears responsibility for confirming to the University contract administrator that the background checks have been completed prior to work being performed by their employees or subcontractors. The Contractor shall only assign to work on the University campus those individuals whom it deems qualified and permissible based on the results of completed background checks. Notwithstanding any other provision herein, and to ensure the safety of students, faculty, staff and facilities, James Madison University reserves the right to approve or disapprove any contract employee that will work on JMU property. Disapproval by the University will solely apply to JMU property and should have no bearing on the Contractor's employment of an individual outside of James Madison University.

P. INDEMNIFICATION: Contractor agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, its officers, agents, and employees from any claims, damages and actions of any kind or nature, whether at law or in equity, arising from or caused by the use of any materials, goods, or equipment of any kind or nature furnished by the contractor/any services of any kind or nature furnished by the contractor, provided that such liability is not attributable to the sole negligence of the using agency or to failure of the using agency to use the materials, goods, or equipment in the manner already and permanently described by the contractor on the materials, goods or equipment delivered.

Q. ADDITIONAL GOODS AND SERVICES: The University may acquire other goods or services that the supplier provides than those specifically solicited. The University reserves the right, subject to mutual agreement, for the Contractor to provide additional goods and/or services under the same pricing, terms, and conditions and to make modifications or enhancements to the existing goods and services. Such additional goods and services may include other products, components, accessories, subsystems, or related services that are newly introduced during the term of this Agreement. Such additional goods and services will be provided to the University at favored nations pricing, terms, and conditions.

R. ADVERTISING: In the event a contract is awarded for supplies, equipment, or services resulting from this proposal, no indication of such sales or services to James Madison University will be used in product literature or advertising without the express written consent of the University. The contractor shall not state in any of its advertising or product literature that James Madison University has purchased or uses any of its products or services, and the contractor shall not include James Madison University in any client list in advertising and promotional materials without the express written consent of the University.

S. ELECTRICAL EQUIPMENT STANDARDS: All equipment/material shall conform to the latest issue of all applicable standards as established by National Electrical Manufacturer's Association (NEMA), American National Standards Institute (ANSI), and Occupational Safety & Health Administration (OSHA). All equipment and material, for which there are OSHA standards, shall bear an appropriate label of approval for use intended from a Nationally Recognized Testing Laboratory (NRTL).

T. CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION: The contractor assures that information and data obtained as to personal facts and circumstances related to faculty, staff, students, and affiliates will be collected and held confidential, during and following the term of this agreement, and will not be divulged without the individual's and the agency's written consent and only in accordance with federal law or the Code of Virginia. This shall include FTI, which is a term of art and consists of federal tax returns and return information (and information derived from it) that is in contractor/agency possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI is categorized as sensitive but unclassified information and may contain personally identifiable information (PII). Contractors who utilize, access, or store personally identifiable information as part of the performance of a contract are required to safeguard this information and immediately notify the agency of any breach or suspected breach in the security of such information. Contractors shall allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting. Contractors and their employees working on this project may be required to sign a confidentiality statement.

U. EXCESSIVE DOWNTIME: Equipment or software furnished under the contract shall be capable of continuous operation. Should the equipment or software become inoperable for a period of more than 24 hours, the contractor agrees to pro-rate maintenance charges to account for each full day of in operability. The period of in operability shall commence upon initial notification. In the event the equipment or software remains inoperable for more than two (2) consecutive calendar days, the contractor shall promptly replace the equipment or software at no charge upon request of the procuring agency. Such replacement shall be with new, unused product(s) of comparable quality, and must be installed and operational within two (2) days following the request for replacement.

V. LATEST SOFTWARE VERSION: Any software product(s) provided under the contract shall be the latest version available to the general public as of the due date of this solicitation.

W. RENEWAL OF MAINTENANCE: Maintenance of the hardware or software specified in the resultant contract may be renewed by the mutual written agreement of both parties for additional one-year periods, under the terms and conditions of the original contract except as noted herein. Price changes may be negotiated at time of renewal; however, in no case shall the maintenance costs for a succeeding one-year period exceed the prior year's contract price(s), increased or decreased by more than the percentage increase or decrease in the other services category of the CPI-W section of the US Bureau of Labor Statistics Consumer Price Index, for the latest twelve months for which statistics are available.

X. SOFTWARE UPGRADES: The Commonwealth shall be entitled to any and all upgraded versions of the software covered in the contract that becomes available from the contractor. The maximum charge for upgrade shall not exceed the total difference between the cost of the Commonwealth's current version and the price the contractor sells or licenses the upgraded software under similar circumstances.

Y. SOURCE CODE: In the event the contractor ceases to maintain experienced staff and the resources needed to provide required software maintenance, the Commonwealth shall be entitled to have, use, and duplicate for its own use, a copy of the source code and associated documentation for the software products covered by the contract. Until such time as a complete copy of such material is provided, the Commonwealth shall have exclusive right to possess all physical embodiments of such contractor owned materials. The rights of the Commonwealth in this respect shall survive for a period of twenty years after the expiration or termination of the contract. All lease and royalty fees necessary to support this right are included in the initial

license fee as contained in the pricing schedule.

Z. THIRD PARTY ACQUISITION OF SOFTWARE: The contractor shall notify the procuring agency in writing should the intellectual property, associated business, or all of its assets be acquired by a third party. The contractor further agrees that the contract's terms and conditions, including any and all license rights and related services, shall not be affected by the acquisition. Prior to completion of the acquisition, the contractor shall obtain, for the Commonwealth's benefit and deliver thereto, the assignee's agreement to fully honor the terms of the contract.

AA. TITLE TO SOFTWARE: By submitting a bid or proposal, the bidder or offeror represents and warrants that it is the sole owner of the software or, if not the owner, that it has received all legally required authorizations from the owner to license the software, has the full power to grant the rights required by this solicitation, and that neither the software nor its use in accordance with the contract will violate or infringe upon any patent, copyright, trade secret, or any other property rights of another person or organization.

BB. WARRANTY AGAINST SHUTDOWN DEVICES: The contractor warrants that the equipment and software provided under the contract shall not contain any lock, counter, CPU reference, virus, worm, or other device capable of halting operations or erasing or altering data or programs. Contractor further warrants that neither it, nor its agents, employees, or subcontractors shall insert any shutdown device following delivery of the equipment and software.

CC. NONVISUAL ACCESS TO TECHNOLOGY: All information technology which, pursuant to this Agreement, is purchased or upgraded by or for the use of any State agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with the following nonvisual access standards from the date of purchase or upgrade until the expiration of this Agreement:

(i) effective, interactive control and use of the Technology shall be readily achievable by nonvisual means;

(ii) the Technology equipped for nonvisual access shall be compatible with information technology used by other individuals with whom any blind or visually impaired user of the Technology interacts;

(iii) nonvisual access technology shall be integrated into any networks used to share communications among employees, program participants or the public; and

(iv) the technology for nonvisual access shall have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

Compliance with the foregoing nonvisual access standards shall not be required if the head of the using agency, institution or political subdivision determines that (i) the Technology is not available with nonvisual access because the essential elements of the Technology are visual and (ii) nonvisual equivalence is not available.

Installation of hardware, software or peripheral devices used for nonvisual access is not required when the Technology is being used exclusively by individuals who are not blind or visually impaired, but applications programs and underlying operating systems (including the format of the data) used for the manipulation and presentation of information shall permit the installation and effective use of nonvisual access software and peripheral devices.

If requested, the Contractor must provide a detailed explanation of how compliance with the foregoing nonvisual access standards is achieved and a validation of concept demonstration.

The requirements of this Paragraph shall be construed to achieve full compliance with the Information Technology Access Act, 2.2-3500 through 2.2-3504 of the *Code of Virginia*.

All information technology which, pursuant to this Agreement, is purchased or upgraded by or for the use of any Commonwealth agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. If requested, the Contractor must provide a detailed explanation of how compliance with Section 508 of the Rehabilitation Act is achieved and a validation of concept demonstration. (http://www.section508.gov/). The requirements of this Paragraph along with the Non-Visual Access to Technology Clause shall be construed to achieve full compliance with the Information Technology Access Act, §§2.2-3500 through 2.2-3504 of the *Code of Virginia.*

DD. OWNERSHIP OF INTELLECTUAL PROPERTY: All copyright and patent rights to all papers, reports, forms, materials, creations, or inventions created or developed in the performance of this contract shall become the sole property of the Commonwealth. On request, the contractor shall promptly provide an acknowledgment or assignment in a tangible form satisfactory to the Commonwealth to evidence the Commonwealth's sole ownership of specifically identified intellectual property created or developed in the performance of the contract.

IX. METHOD OF PAYMENT

The contractor will be paid on the basis of invoices submitted in accordance with the solicitation and any negotiations. James Madison University recognizes the importance of expediting the payment process for our vendors and suppliers; however, vendor enrollment for E-Payments has temporarily been suspended as we transition to a new bank. Once we are operational with our new bank, we will ask that our vendors and suppliers enroll in our bank's single use Commercial Card Number process or electronic deposit (ACH) to your bank account so that future payments are made electronically. Contractors signed up for the single use Commercial Card Number process will receive the benefit of being paid in Net 15 days. Additional information is available online at: http://www.jmu.edu/financeoffice/accounting-operations-disbursements/cash-investments/vendor-payment-methods.shtml

X. PRICING SCHEDULE

The offeror shall provide pricing for all products and services included in proposal indicating one-time and on-going costs. The resulting contract will be cooperative per item VIII. K.

Providing pricing for items requested in I.V. Statement of Needs, including but not limited to potential costs listed below:

A. Licensing model and pricing including, as relevant, breakdown by modules, user volume, pricing tiers, and/or discounts available to JMU and VASCUPP members who may utilize any resulting cooperative contract.

B. Provide price for product and services including a total project cost.

a. Provide breakdown of base pricing and separate optional module costs.

b. Provide breakdown of hardware costs (indicate required and optional devices as relevant).

C. Implementation Services, include expenses breakdown, (personnel/days/hours).

a. Price any on premises hourly rates to be inclusive of travel costs.

b. Data migration costs.

D. Customization and Configuration Cost

E. Ongoing Maintenance and Support

F. Integrations

G. Initial and Ongoing Training

a. Price any on premises hourly rates to be inclusive of travel costs.

H. Professional Services

I. All Other Cost (including optional costs)

J. Specify any associated charge card processing fees, if applicable, to be billed to the university. Vendors shall provide their VISA registration number when indicating charge card processing fees. Any vendor requiring information on VISA registration may refer to https://usa.visa.com/support/small-business/regulations-fees.html and for questions https://usa.visa.com/dam/VCOM/global/support-legal/documents/merchant-surcharging-qa-for-web.pdf.

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

Attachment B: Small, Women, and Minority-owned Business (SWaM) Utilization Plan

Attachment C: Standard Contract Sample

Attachment D: Information Technology Services Addendum ***(All Offerors are required to complete)***

Attachment E: Commonwealth of Virginia Agency Contract Form Addendum to Contractor's Form ***(All Offerors are required to complete)***

Attachment F: Higher Education Cloud Assessment Tool (HECVAT) - attached as a separate Excel spreadsheet ***(All Offerors are required to complete)***

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years_____ Months_____

3. REFERENCES: Indicate below a listing of at least five (5) organizations, either commercial or governmental/educational, that your agency is servicing. Include the name and address of the person the purchasing agency has your permission to contact.

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

4. List full names and addresses of Offeror and any branch offices which may be responsible for administering the contract.

_____

_____

_____

_____

5. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
   [ ] YES [ ] NO
   IF YES, EXPLAIN:_____

_____

_____

_____

ATTACHMENT B

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Offeror Name: _____ Preparer Name: _____

Date: _____

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes____ No_____

If yes, certification number: _____ Certification date:_____

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes_____ No_____

If yes, certification number: _____ Certification date: _____

Instructions: *Populate the table below to show your firm's plans for utilization of small, women-owned and minority-owned business enterprises in the performance of the contract. Describe plans to utilize SWAMs businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc.*

Small Business: "Small business " means a business, independently owned or operated by one or more persons who are citizens of the United States or non-citizens who are in full compliance with United States immigration law, which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of $10 million or less averaged over the previous three years.

Woman-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified women-owned businesses are also a small business enterprise.**

Minority-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified minority-owned businesses are also a small business enterprise.**

Micro Business is a certified Small Business under the SWaM Program and has no more than twenty-five (25) employees **AND** no more than $3 million in average annual revenue over the three-year period prior to their certification.

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Small Business and Supplier Diversity (SBSD) to be counted in the SWAM program. Certification applications are available through SBSD at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at http://www.sbsd.virginia.gov/ (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Procurement Name and Number: _____ Date Form Completed:_____

Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses
for this Proposal and Subsequent Contract

Offeror / Proposer:

Firm	Address	Contact Person/No.
_____	_____	_____

Sub-Contractor's Name and Address	Contact Person & Phone Number	SBSD Certification Number	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to date (to be submitted with request for payment from JMU)

(Form shall be submitted with proposal and if awarded, again with submission of each request for payment)

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No._____

This contract entered into this_____day of_____20____,by _____ hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

WITNESSETH that the Contractor and the Purchasing Agency, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

SCOPE OF CONTRACT: The Contractor shall provide the services to the Purchasing Agency as set forth in the Contract Documents.

PERIOD OF PERFORMANCE: From_____ through_____

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposals dated _____:
- (a) The Statement of Needs,
- (b) The General Terms and Conditions,
- (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
- (d) List each addendum that may be issued

(3) The Contractor's Proposal dated _____and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations summary dated _____.

SAMPLE

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

CONTRACTOR:	PURCHASING AGENCY:
By:_____	By:_____
(Signature)	(Signature)
_____	_____
(Printed Name)	(Printed Name)
Title:_____	Title:_____

ATTACHMENT D

James Madison University
Information Technology Services Addendum

CONTRACTOR NAME: _____

PRODUCT/SOLUTION: _____

Definitions:

- Agreement: The "Agreement" includes the contract, this addendum and any additional addenda and attachments to the contract, including the Contractor's Form.
- University: "University" or "the University" means James Madison University, its trustees, officers and employees.
- University Data: "University Data" is defined as any data that the Contractor creates, obtains, accesses, transmits, maintains, uses, processes, stores or disposes of in performance of the Agreement. It includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites.
- Personally Identifiable Information: "Personally Identifiable Information" (PII) includes but is not limited to: Any information that directly relates to an individual and is reasonably likely to enable identification of that individual or information that is defined as PII and subject to protection by James Madison University under federal or Commonwealth of Virginia law.
- Security Breach: "Security Breach" means a security-relevant event in which the security of a system or procedure involving University Data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
- Service(s): "Service" or "Services" means any goods or services acquired by the University from the Contractor.

1. **Rights and License in and to University Data:** The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Contractor has a limited, nonexclusive license to use the data as provided in the Agreement solely for the purpose of performing its obligations hereunder. The Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property.

2. **Disclosure:** All goods, products, materials, documents, reports, writings, video images, photographs, or papers of any nature including software or computer images prepared or provided to the Contractor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.

3. **Data Privacy:**
   a. Contractor will use University Data only for the purpose of fulfilling its duties under the Agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by law.
   b. University Data will not be stored outside the United States without prior written consent from the University.
   c. Contractor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill obligations under the Agreement. The Contractor will ensure that the Contractor's employees, and subcontractors when applicable, who perform work under the Agreement have received appropriate instruction as to how to comply with the data protection provisions of the Agreement and have agreed to confidentiality obligations at least as restrictive as those contained in this Addendum.

i. If the Contractor will have access to the records protected by the Family Educational Rights and Privacy Act (FERPA), Contractor acknowledges that for the purposes of the Agreement it will be designated as a "school official" with "legitimate educational interests" in such records, as those terms have been defined under FERPA and its implementing regulations, and Contractor agrees to abide by the limitations and requirements imposed on school officials. Contractor will use such records only for the purpose of fulfilling its duties under the Agreement for University's and its End Users' benefit, and will not share such data with or disclose it to any third party except as required by law or authorized in writing by the University. Contractor acknowledges that its access to such records is limited to only those directly related to and necessary for the completion of Contractor's duties under the Agreement.

d. The Contractor shall be responsible and liable for the acts and omissions of its subcontractors, including but not limited to third-party cloud hosting providers, and shall assure compliance with the requirements of the Agreement.

4. **Data Security:**
   a. Contractor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.
   b. Contractor will store and process University Data in a secure site and will provide a SOC 2 or other security report deemed sufficient by the University from a third party reviewer along with annual updated security reports. If the Contractor is using a third-party cloud hosting company such as AWS, Rackspace, etc., the Contractor will obtain the security audit report from its hosting company and give the results to the University. The University should not have to request the report directly from the hosting company.
   c. Contractor will use industry-standards and up-to-date security tools, technologies and practices such as network firewalls, anti-virus, vulnerability scans, system logging, intrusion detection, 24x7 system monitoring, and third-party penetration testing in providing services under the Agreement.
   d. Without limiting the foregoing, Contractor warrants that all electronic University Data will be encrypted in transmission (including via web interface) and stored at AES 256 or stronger.

5. **Data Authenticity, Integrity and Availability:**
   a. Contractor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. Contractor shall be responsible for ensuring that University Data, per the Virginia Public Records Act, is "preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic records as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration."
   b. Contractor will ensure backups are successfully completed at the agreed interval and that restoration capability is maintained for restoration to a point-in-time and\or to the most current backup available.
   c. Contractor will maintain an uptime of 99.99% or greater as agreed to for the contracted services via the use of appropriate redundancy, continuity of operations and disaster recovery planning and implementations, excluding regularly scheduled maintenance time.

6. **Employee Background Checks and Qualifications:**
   a. Contractor shall ensure that its employees have undergone appropriate background screening and possess all needed qualifications to comply with the terms of the Agreement including but not limited to all terms relating to data and intellectual property protection.
   b. If the Contractor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data, the Contractor shall perform the following background checks on all employees who

have potential to access such data in accordance with the Fair Credit Reporting Act: Social Security Number trace; seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes; Office of Foreign Assets Control List (OFAC) check; Bureau of Industry and Security List (BIS) check; and Office of Defense Trade Controls Debarred Persons List (DDTC).

7. **Security Breach:**
   a. Response: Immediately (within one day) upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of University Data, Contractor will notify the University ISO at (ISO@jmu.edu), fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Contractor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.
   b. Liability:
      i. If Contractor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Contractor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security Breach caused by Contractor, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.
      ii. If Contractor will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Contractor will reimburse the University in full for all costs reasonably incurred by the University in investigation and remediation of any Security Breach caused by Contractor.

8. **Requests for Data, Response to Legal Orders or Demands for Data:**
   a. Except as otherwise expressly prohibited by law, Contractor will:
      i. immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking University Data;
      ii. consult with the University regarding its response;
      iii. cooperate with the University's requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and
      iv. Upon the University's request, provide the University with a copy of its response.
   b. Contractor will make itself and any employees, contractors, or agents assisting in the performance of its obligations under the Agreement, available to the University at no cost to the University based upon claimed violation of any laws relating to security and\or privacy of the data that arises out of the Agreement. This shall include any data preservation or eDiscovery required by the University.
   c. The University may request and obtain access to University Data and related logs at any time for any reason and at no extra cost.

9. **Data Transfer Upon Termination or Expiration:**
   a. Contractor's obligations to protect University Data shall survive termination of the Agreement until all University Data has been returned or securely destroyed, meaning taking actions that render data written on media unrecoverable by both ordinary and extraordinary means.
   b. Upon termination or expiration of the Agreement, Contractor will ensure that all University Data are securely transferred, returned or destroyed as directed by the University in its sole discretion within

60 days of termination of the Agreement. Transfer/migration to the University or a third party designated by the University shall occur without significant interruption in service. Contractor shall ensure that such transfer/migration uses facilities, methods, and data formats that are accessible and compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition.

c. In the event that the University requests destruction of its data, Contractor agrees to securely destroy all data in its possession and in the possession of any subcontractors or agents to which Contractor might have transferred University data. Contractor agrees to provide documentation of data destruction to the University.
d. Contractor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Contractor's facilities to remove and destroy University-owned assets and data. Contractor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. The Contractor will also provide, as applicable, a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. Contractor will work closely with its successor to ensure a successful transition to the new service, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

10. **Audits:**
    a. The University reserves the right in its sole discretion to perform audits of the Contractor to ensure compliance with the terms of the Agreement. Contractor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which Contractor must create, obtain, transmit, use, maintain, process, or dispose of University Data.
    b. If Contractor must under the Agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data, Contractor will at its expense conduct or have conducted at least annually a(n):
        i. American Institute of CPAs Service Organization Controls 2 (SOC 2) audit, or other independent security audit with audit objectives deemed sufficient by the University, which attests to Contractor's security policies, procedures, and controls. Contractor shall also submit such documentation for any third-party cloud hosting provider(s) they may use (e.g. AWS, Rackspace, Azure, etc.) and for all subservice providers or business partners relevant to the Agreement. Contractor shall also provide James Madison University with a designated point of contact for the SOC reports and risks related to the contract. This person shall address issues raised in the SOC reports of the Contractor and its relevant providers and partners, and respond to any follow up questions posed by the University in relation to technology systems, infrastructure, or information security concerns related to the contract.
        ii. vulnerability scan of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement; and
        iii. formal penetration test performed by qualified personnel of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under the Agreement.
    c. Additionally, Contractor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under the Agreement. The University may require, at University expense, the Contractor to perform additional audits and tests, the results of which will be provided promptly to the University.

11. **Compliance:**
    a. Contractor will comply with all applicable laws and industry standards in performing services under the Agreement. Any Contractor personnel visiting the University's facilities will comply with all

applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Contractor upon request.

b. To the extent applicable to the design and intended use of the service, Contractor warrants that the service it will provide to the University is fully compliant with and will enable the University to be compliant with relevant requirements of all laws, regulation, and guidance applicable to the University and/or Contractor, including but not limited to: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.

12. **No End User Agreements:** Any agreements or understandings, whether electronic, click through, verbal or in writing, between Contractor and University employees or other end users under the Agreement that conflict with the terms of the Agreement, including but not limited to this Addendum, shall not be valid or binding on the University or any such end users.

IN WITNESS WHEREOF, the parties have caused this addendum to be duly executed, intending thereby to be legally bound. In the event of conflict or inconsistency between terms of the Agreement and this Addendum, the terms of this Addendum shall prevail.

JAMES MADISON UNIVERSITY		**CONTRACTOR**	
SIGNATURE:	_____	SIGNATURE:	_____
PRINTED NAME:	_____	PRINTED NAME:	_____
TITLE:	_____	TITLE:	_____
DATE:	_____	DATE:	_____

REV: March 23, 2020

ATTATCHMENT E

COMMONWEALTH OF VIRGINIA AGENCY
CONTRACT FORM ADDENDUM TO CONTRACTOR'S FORM

AGENCY NAME: **James Madison University**

CONTRACTOR NAME: _____

DATE: _____

The Commonwealth and the Contractor are this day entering into a contract and, for their mutual convenience, the parties are using the standard form agreement provided by the Contractor. This addendum, duly executed by the parties, is attached to and hereby made a part of the contract. In the event that the Vendor enters into terms of use agreements or other agreements of understanding with University employees and students (whether electronic, click-through, verbal, or in writing), the terms and conditions of this Agreement shall prevail.

The Contractor represents and warrants that it is a(n) / / individual proprietorship / / association / / partnership / / corporation / / governmental agency or authority authorized to do in Virginia the business provided for in this contract. (**Check the appropriate box.)**

Notwithstanding anything in the Contractor's form to which this Addendum is attached, the payments to be made by the Commonwealth for all goods, services and other deliverables under this contract shall not exceed Purchase Order Amounts; payments will be made only upon receipt of a proper invoice, detailing the goods/services provided and submitted to James Madison University. The total cumulative liability of the Commonwealth, its officers, employees and agents in connection with this contract or in connection with any goods, services, actions or omissions relating to the contract, shall not under any circumstance exceed payment of the above maximum purchase price plus liability for an additional amount equal to such maximum purchase price. In its performance under this contract, the Contractor acts and will act as an independent contractor, and not as an agent or employee of the Commonwealth.

The Contractor's form contract is, with the exceptions noted herein, acceptable to the Commonwealth. Nonetheless, because certain standard clauses that may appear in the Contractor's form agreement cannot be accepted by the Commonwealth, and in consideration of the convenience of using that form, and this form, without the necessity of specifically negotiating a separate contract document, the parties hereto specifically agree that, notwithstanding any provisions appearing in the attached Contractor's form contract, none of the following paragraphs **1 through 18** shall have any effect or be enforceable against the Commonwealth:

1. **Requiring the Commonwealth to maintain any type of insurance either for the Commonwealth's benefit or for the contractor's benefit;**

2. **Renewing or extending the agreement beyond the initial term or automatically continuing the contract period from term to term;**

3. **Requiring or stating that the terms of the attached Contractor's form agreement shall prevail over the terms of this addendum in the event of conflict;**

4. **Requiring the Commonwealth to indemnify or to hold harmless the Contractor for any act or omission;**

5. **Imposing interest charges contrary to that specified by the *Code of Virginia*, §2.2-4347 through 2.2-4354, Prompt Payment;**

6. **Requiring the application of the law of any state other than Virginia in interpreting or enforcing the contract or requiring or permitting that any dispute under the contract be resolved in the courts of any state other than Virginia;**

7. **Requiring any total or partial compensation or payment for lost profit or liquidated damages by the Commonwealth if the contract is terminated before its ordinary period;**

8. **Requiring that the contract be "accepted" or endorsed by the home office or by any other officer subsequent to execution by an official of the Commonwealth before the contract is considered in effect;**

9. **Delaying the acceptance of this contract or its effective date beyond the date of execution;**

10. **Limiting or adding to the time period within which claims can be made or actions can be brought;**

11. **Limiting the liability of the Contractor for property damage or personal injury. The parties agree that this clause does not extend the Contractor's liability beyond its own acts or those of its agents/employees;**

12. **Permitting unilateral modification of this contract by the Contractor;**

13. **Binding the Commonwealth to any arbitration or to the decision of any arbitration board, commission, panel or other entity;**

14. **Obligating the Commonwealth to pay costs of collection or attorney's fees;**

15. **Granting the Contractor a security interest in property of the Commonwealth;**

16. **Bestowing any right or incurring any obligation that is beyond the duly granted authority of the undersigned agency representative to bestow or incur on behalf of the Commonwealth.**

17. **Requiring the "confidentiality" of the agreement, in whole or part, without (i) invoking the protection of Section 2.2-4342F of the Code of Virginia in writing prior to signing the agreement (ii) identifying the data or other materials to be protected, and (iii) stating the reasons why protection is necessary.**

18. **Requiring the Commonwealth to reimburse for travel and living expenses in excess of the agency policy located at** https://www.jmu.edu/financemanual/procedures/4215mie.shtml

This contract has been reviewed by staff of the agency. Its substantive terms are appropriate to the needs of the agency and sufficient funds have been allocated for its performance by the agency. This contract is subject to appropriations by the Virginia General Assembly.

IN WITNESS WHEREOF, the parties have caused this contract to be duly executed, intending thereby to be legally bound.

AGENCY by _____ **CONTRACTOR by** _____

Title _____ **Title** _____

Printed Name _____ **Printed Name** _____

April. 2017

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 Cloud Vendor Assessment Tool** (**HECVAT**) attempts to generalize higher education information security and data protection questions and issues for consistency and ease of use. Some institutions may have specific issues that must be addressed in addition to the general questions provided in this assessment. It is anticipated that this HECVAT will be revised over time to account for changes in cloud services provisioning and the information security and data protection needs of higher education institutions.

The Higher Education Cloud Vendor Assessment Tool:
- Helps higher education institutions ensure that cloud 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 cloud services without increasing risks
- Reduces the burden that cloud service providers face in responding to requests for security assessments from higher education institutions

The HECVAT 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 third-party provided cloud 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 2018
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 Tool 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 Cloud Vendor Assessment Tool - 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 Cloud Vendor Assessment Tool, 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 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 Cloud Vendor Assessment Tool

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.	

For Institution's Security Analysts
Raw vendor answers can be viewed in the Cloud Vendor Assessment Tool tab. 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. Select complaince 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. 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 Cloud Vendor Assessment Tool				Version 2.03
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 Cloud Vendor Assessment Tool (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	*James Madison University is located in Harrisonburg, VA; our data zone is the Contiguous United States (CONUS)*		
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 Cloud Vendor Assessment Tool (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?	Yes		You are required to complete the questions in the HIPAA section.
QUAL-02	Does the vended product host/support a mobile application? (e.g. app)	Yes		You are required to complete the questions in the Mobile Application section.
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)	Yes		You are required to complete the questions in the Third Parties section.

QUAL-04	Do you have a Business Continuity Plan (BCP)?	Yes		You are required to complete the questions in the Business Continuity section.
QUAL-05	Do you have a Disaster Recovery Plan (DRP)?	Yes		You are required to complete the questions in the Disaster Recovery section.
QUAL-06	Will data regulated by PCI DSS reside in the vended product?	Yes		You are required to complete the questions in the PCI DSS section.
QUAL-07	Is your company a consulting firm providing only consultation to the Institution?	No		Responses to the questions in the Consulting section are optional.
Documentation		**Vendor Answers**	**Additional Information**	**Guidance**
DOCU-01	Have you undergone a SSAE 16 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 - Optional based on QUALIFIER response.		**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 adminstrative 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	Does the system provide data input validation and error messages?			
APPL-18	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 network-based Intrusion Detection System?			

FIDP-06	Have you implemented an network-based Intrusion Prevention System?			
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 addtion 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 defined)
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?	No		Describe your intent to implement physical security controls and policies.
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

EDUCAUSE

Acknowledgments

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

Members that contributed to Phase III (2018) of this effort are:
- Jon Allen, Baylor University
- Josh Callahan, Humbolt 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
- 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

contributed their
.