Request for Proposals

Issue Date:	April 1, 2025
RFP Number:	VCCS-WIDE-25-88416
Title:	Course Development Authoring Tool
Commodity Code:	20987 – Software, Mini/Mainframe Computer (Not Otherwise Classified) 92416 – Course Development Services, Instructional/Training 98574 – Software, Computer, Rental or Lease
Issuing Agency:	Commonwealth of Virginia Virginia Community College System - Shared Services Center 147 Daleville Centre Drive Daleville, Virginia 24083

Contract Term: Two (2) years with four (4) two-year renewals, at VCCS's sole option, or as negotiated.

Proposals will be Received Until: **May 9th, 2025, at 5:00 PM local time.**

All Proposals must be received in eVA by the date and time stated immediately above. Any Proposals received after the stated time and date will not be considered.

In lieu of a Pre-Proposal Conference, questions will be accepted by e-mail to Aubrey Wilcher through April 16th, 2025, at 5:00 pm EST.

Any inquiries regarding this solicitation should be directed only to:
Aubrey Wilcher, Senior Contract Officer
Email: awilcher@ssc.vccs.edu

All inquiries must be made in writing and must be submitted electronically as indicated in the RFP. No oral inquiries will be accepted. From the date of issuance of this RFP, until the selection of a Contractor(s) is announced, all questions concerning any part of this RFP shall be directed ONLY to Aubrey Wilcher (awilcher@ssc.vccs.edu). It is not permissible for an Offeror, or any entity working on behalf of an Offeror, to solicit information from any individual or government source (Federal or State) other than from the official point of contact listed above. Any unauthorized solicitations for information are grounds for disqualification of Offeror's proposal.

In compliance with this Request for Proposals (RFP) and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods and services in accordance with the attached submitted proposal or as mutually agreed upon by subsequent negotiation.

Legal Name of Firm:	Date:
Address of Firm:	By:
eVA Vendor ID Number:	Name:
DSBSD Certification Number:	Title:
Phone:	Email:

Note: This public body does not discriminate against faith-based organizations in accordance with the Code of Virginia, § 2.2-4343.1 or against a bidder or offeror because of race, religion, color, sex, national origin, age, disability, sexual orientation, gender identity, political affiliation, or veteran status or any other basis prohibited by state law relating to discrimination in employment. Faith-based organizations may request that the issuing agency not include subparagraph 1.e in General Terms and Condition C. Such a request shall be in writing and explain why an exception should be made in that invitation to bid or request for proposal

Table of Contents

*** These items must be completed and returned as part of the RFP submission package.*

I. PURPOSE

The purpose of this Request for Proposals (RFP) is to solicit sealed proposals from qualified offerors to establish one or more contracts through competitive negotiation for a Commercial off the Shelf (COTS) course development authoring tool. The VCCS invites any qualified offeror to respond to this RFP by submitting a proposal for such work, services, and/or items consistent with the terms and conditions set forth herein.

This procurement is being conducted on behalf of the Virginia Community College System (VCCS). The VCCS consists of 23 colleges with 40 campuses located across the state, as well as two central agencies: the System Office and Shared Services Center. **Each of these VCCS entities may use any awarded contract at their option. However, they are under no obligation to do so, and there is no guarantee that any awarded contractor shall receive a request for product or services from any of the 23 colleges, the System Office or the Shared Services Center.**

II. BACKGROUND

The Virginia Community College System (VCCS) consists of 23 community colleges across the Commonwealth of Virginia. Student populations range in size from 1,000 students to 100,000 students per college. Virginia's community colleges serve an estimated 250,000 students per year total.

III. STATEMENT OF NEEDS

The Successful Offeror shall furnish all services including, but not limited to, providing the necessary labor, materials, supervision, equipment, services, incidentals, and related items necessary to provide a Commercial-off-the-Shelf (COTS) course development authoring tool that supports the creation of interactive and engaging courses.

The Successful Offeror shall meet the required qualifications that follow:

1. **SPECIFIC SERVICES:**

a) Allows for the development of highly interactive and engaging content for online, hybrid, and classroom formats

   i. The ability to utilize videos, audio, animations, and graphics

   ii. Create templates for multiple uses

   iii. Ability to insert logos and images

   iv. Features for creating custom interactions, branching scenarios, simulations, gamification elements, drag-and-drop activities, quizzes, assessments, etc.

b) Ability to create courses that are fully responsive and accessible on various devices, including desktops, tablets, and smartphones

c) Interface that can be easily used by users of varying levels of technical expertise

d) Access to templates and pre-built assets to streamline the course development process

e) Has the ability to allow collaboration among different creators

f) Tools for collecting and managing feedback during the course development process

g) Provides access to comprehensive training resources, including live webinars, on-demand tutorials, live support, and support community

h) Compatibility with Canvas LMS

i) Analytics to track progress and performance

j) Support for creating courses in multiple languages

k) Capability to reuse and repurpose created content across different courses.

l) Explain the implementation process. What steps are your responsibility, and which are those of the VCCS?

m) Describe how your solution scales to accommodate increasing workloads and user demands. Including:

   i. The maximum number of users your solution can support simultaneously

   ii. How is performance maintained as the number of users or data volume increase?

   iii. Do you have any built-in features that facilitate scalability, such as load balancing or auto-scaling?

   iv. Provide examples of how your solution has scaled in real-world scenarios.

2. TECHNICAL REQUIREMENTS:

Any proposed solution must address and/or provide the following technical requirements to include, but not limited to the following:

a) Describe what data is stored in your product and any data disposition and backup processes.

   a. Specify data exportability and portability. Can data be transferred from another system, if needed?

b) Provide the average initial set-up time (installation and configuration) for the system.

c) Describe the institutional hardware requirements for VCCS for your product.

d) Provide a detailed description of the software upgrade methodology. How often is the software updated and how do these updates impact service?

e) Provide a detailed description of the approach to provisioning and managing software licenses on this project. Provide a copy of the license agreement(s).

f) Describe how your company prevents system outages and ensures maximum uptime for the system.

g) Describe how your company intends on complying with all VCCS IT privacy requirements and the data security requirements outlined in Attachment 7 "VCCS Cloud Service Provider Security Requirements" including confirmation of your company's SOC 2 Type II certification or equivalent.

h) Identify your hosting environment and provide any supporting information for 3rd party hosts including confirmation of a SOC 2 Type II Certification or equivalent.

   a. **Note: SOC 2 Type II Certification equivalent is (a) The Federal Risk and Authorization Management Program (FedRAMP), or (b) ISO3000 Type 2 Certifications.**

i) Describe how your company intends on providing for disaster recovery of all system data.

j) Describe how segregation of duties is maintained using a Role Based Access model and the various roles for users supported by your solution. Indicate which roles are exclusive to your personnel, which roles are exclusive to VCCS users, and which of these roles have elevated privileges that allow modification of user role assignments within your solution. The solution should allow centralized administration of a multi-tenant segregated environment such that college users can only access personnel assigned to their respective college with central administration having access to all employee data across the enterprise.

k) The vendor must ensure that any AI software adheres to the following standards and practices:

   a. Ethical AI Usage: The software must be designed and implemented in a manner that ensures ethical use of AI, avoiding biases and ensuring fairness in decision making processes.

   b. Transparency and Accountability: The vendor must provide clear documentation on how AI algorithms are developed, trained, and deployed. This includes information on data sources, model training processes, and decision-making criteria.

   c. Data Privacy and Security: The software must comply with all relevant data privacy regulations, including GDPR and CCPA. The vendor must implement robust security measures to protect sensitive data from unauthorized access and breaches.

   d. Regular Updates and Improvements: The vendor must commit to regularly updating the software to incorporate the latest advancements in AI technologies and address any discovered vulnerabilities. This includes providing detailed document of updates and their impact on the system.

   e. Bias Mitigation: The vendor must implement measures to identify and mitigate biases in AI algorithms. This includes regular audits and assessments to ensure that the software remains unbiased and fair.

f. Compliance with Regulatory Standards: The software must comply with all relevant regulatory standards and guidelines for AI usage, including those related to algorithm transparency and data privacy.

g. Performance and Reliability: The vendor must ensure that the AI algorithms used in the software are accurate, reliable, and robust, minimizing the risk of errors and operational failures.

h. Ethical Considerations: The vendor must address ethical concerns related to AI usage, including the potential for misuse and the impact on user trust. This includes implementing safeguards to prevent malicious or unethical use of the software.

l) Accessibility Requirements

a. Compliance with WCAG 2.1 AA or higher

b. Support for screen readers, keyboard navigation, and closed captions

c. Automated accessibility checks withing the platform

d. Ability to create accessible interactions (i.e. drag-and-drop with keyboard alternatives)

e. Support for alternative text descriptions for media.

m) Describe if/how your solution will support the following VCCS information security requirements for user authorization and authentication:

VCCS Staff Authentication

- SAML 2.x or OpenID connect for VCCS staff authentication. VCCS uses single-sign-on as its Identity provider
- Must have just in-time provisioning
- Must allow for provisioning of accounts using SCIM provisioning

VCCS Staff Authorization

- Security authorization must be managed using Identity management system (SAML Claims, or OpenID claims)

3. SERVICE LEVEL AGREEMENT

A Service Level Agreement (SLA) must be developed by the contractor, in coordination with the VCCS and the express concept that the SLA must be acceptable to the VCCS and their appointed counsel from the Office of the Attorney General. The SLA shall include a description of the products and/or services provided, levels of acceptable services, verifiable performance criteria, their monitoring and reporting and remedies. The VCCS retains the right to monitor and revoke any activity related to its assets. The VCCS retains the right to audit responsibilities defined in any resulting contract or agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors.

a) Describe the methodology and process for identifying performance criteria, levels of acceptable service and monitoring and reporting activities.

b) Define the metrics for integration transaction success and cycle times; uptime and maximum downtimes; and meantime to repair.

c) Describe how your company intends on providing technical support via telephone and email and identify error levels and response times.

d) Provide a draft SLA that incorporates performance commitments, obligations, and expectations.

e) Describe the methodology and process for establishment of an escalation process for problem resolution.

f) Describe the methodology, performance metrics, expectations, and obligations for performance regarding customer service and help desk activities.

IV. COMPLIANCE

A. The Selected Firm/Vendor will comply with all applicable laws and industry standards in performing services under this agreement. Any Selected Firm/Vendor personnel visiting College facilities will comply with all applicable Virginia Community College System and College policies regarding access to, use of, and conduct within such facilities. The College will provide copies of such policies to the Selected Firm/Vendor upon request.

B. Selected Firm/Vendor warrants that the service it will provide to the College is fully compliant with all state and federal laws, regulations, industry codes, and guidance that may be applicable to the service, which may include:

1. Any applicable national, federal, state or local law, rule, directive or regulation relating to the privacy of personal information, including without limitation, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g, and its implementing regulations ("FERPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Privacy and Security Rules issued thereunder, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), the Financial Modernization Act of 1999 ("Gramm-Leach-Bliley Act"), the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act, the Americans with Disabilities Act, and the Virginia Consumer Data Protection Act;

2. Any privacy policy or practice applicable to any personal information that Customer or any User accesses, uses, colleges, or maintains hereunder, including, without limitation any practice required in connection with the processing of credit card data, including the Payment Card Industry Data Security Standards (PCI-DSS); and

3. Federal Export Administration Regulations, Federal Acquisitions Regulations, Defense Federal Acquisitions Regulation and Department of Education guidance.

C. If the Payment Card Industry Data Security Standard (PCI-DSS) is applicable to the Selected Firm/Vendor service provided to the College, the Selected Firm/Vendor agrees to:

1. Store, transmit, and process College Data in scope of the PCI DSS in compliance with the PCI DSS;

2. Attest that any third-party providing services in scope of PCI DSS under this agreement will store, transmit, and process College Data in scope of the PCI DSS in compliance with the PCI DSS;

3. Provide either proof of PCI DSS compliance or a certification (from a recognized third-party security auditing firm), within 10 business days of the request, verifying Firm/Vendor and any third party who stores, transmits, or processes College Data in scope of the PCI DSS as part of the services provided under this agreement maintains ongoing compliance under PCI DSS as it changes over time;

4. Store, transmit, and process any College Data in scope of the PCI DSS in a manner that does not bring the College's network into PCI DSS scope; and

5. Attest that any third-party providing services in scope of PCI DSS under this agreement will store, transmit, and process College Data in scope of the PCI DSS in a manner that does not bring the College's network into PCI DSS scope.

V. PROPOSAL ADMINISTRATION AND INSTRUCTIONS

A. Overview - This RFP was developed to provide all potential Suppliers with the information required to prepare proposals. This section outlines the administrative procedures and guidelines you must use and comply with when preparing a proposal. Nothing in this RFP constitutes an offer or an invitation to a contract.

C. **Virginia Public Procurement Act (VPPA) -** This RFP is governed by the Virginia Public Procurement Act ("VPPA"), Code § 2.2-4300 *et seq*., and other applicable laws.

D. **Anti-Discrimination- § 2.2-4310 and § 2.2-4311, and § 2.2-4343.1(E) -** By submitting its proposal, a Supplier certifies to the Commonwealth that it 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; and, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and § 2.2-4311 of the VPPA.

E. **Ethics in Public Contracting - § 2.2-4367 *et seq*. -** By submitting its proposal, a Supplier certifies that its proposal is made without collusion or fraud; that the Supplier has not offered or received any kickbacks or inducements from any other bidder, supplier, manufacturer, or subcontractor in connection with its proposal; and that the Supplier has 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. In addition, a Supplier

will disclose any actual or perceived conflicts of interest in its proposal and will notify VCCS if it becomes aware of a potential conflict of interest in the future.

F. **Announcement of Award - § 2.2-4300 *et seq*. -** If a contract is awarded or announced as a result of this RFP, the purchasing agency will post notice of the award decision on the DGS/DPS eVA web site (http://www.eva.virginia.gov) for a minimum of 10 days. No award decision will be provided verbally. Any final contract, including pricing, awarded as a result of this RFP will be made available for public inspection.

G. **Authorization to Transact Business in the Commonwealth - § 2.2-4311.2 -** All Suppliers organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership, or registered as a registered limited liability partnership must be authorized to transact business as a domestic or foreign business entity if so required by Title 13.1 or Title 50 of the Code, or as otherwise required by law. In its proposal, Supplier must include either (i) Supplier's identification number issued to it by the State Corporation Commission; or (ii) a statement explaining why Supplier is not required to be registered. No award can be made to any Supplier without this information unless this requirement is waived. Appendix D of this solicitation includes a space for Supplier to provide the information required in (i) or (ii) of this subsection. If a Supplier anticipates the use of additional resources through a partnership or subcontracting relationship with other entities, the requirements of this Section 2.F will also apply to any entities that are engaged as partners or subcontractors of Supplier providing services directly to the Commonwealth upon award of a contract.

H. **Prohibited Products and Services - § 2.2-5514 -** No Supplier may include as part of its proposal, whether directly or indirectly through subcontractors, any hardware, software, or services that have been prohibited for use on federal systems by the U.S. Department of Homeland Security.

I. **Prohibited Contributions and Gifts - § 2.2-4376.1 -** No Supplier that submits a proposal in response to this solicitation, and no individual who is an officer or director of the Supplier shall knowingly provide a contribution, gift, or other items or make an express or implied promise to make such a contribution or gift to the Governor, his political action committee, or the Secretary of Administration during the period between the submission of the proposal and the award of any resulting contract award with an expected value of $5 million or more dollars.

J. **Liability -** The issuance of this RFP and the receipt of information in response to this RFP will not cause VCCS to incur any liability or obligation, financial or otherwise, to any Supplier. VCCS assumes no obligation to reimburse or in any way compensate a Supplier for expenses incurred in connection with its proposal.

K. **Disclosure -** Except as provided in paragraph "K" below, all proceedings, records, contracts and other public records relating to this procurement shall be open to the inspection of any citizen, or any interested person, firm or corporation, in accordance with the Virginia Freedom of Information Act (§ 2.2-3700 et seq.)

L. **Trade Secrets and Proprietary Information -** FAILURE TO COMPLY WITH THE FOLLOWING STATUTORY REQUIREMENTS WILL RESULT IN ALL PROPOSAL MATERIALS BEING SUBJECT TO RELEASE TO OTHER OFFERORS AND THE PUBLIC IN ACCORDANCE WITH THE VPPA AND THE VIRGINIA FREEDOM OF INFORMATION ACT.

Pursuant to Code § 2.2-4342(F), trade secrets or proprietary information submitted by a bidder or offeror in connection with a procurement transaction (or, if applicable, a prequalification application submitted pursuant to subsection B of § 2.2-4317) shall not be subject to the Virginia Freedom of Information Act (Code § 2.2- 3700 *et seq*.) ***if*** a Supplier:

i). invokes the protections of this section in writing prior to or upon submission of the data or other materials,
ii). identifies specifically the data or other materials to be protected, and
iii). states the reasons why protection is necessary.

Please note that you may not designate as trade secrets or proprietary information (a) an entire bid, proposal, or prequalification application; (b) any portion of a bid, proposal, or prequalification application that does not contain trade secrets or proprietary information; or (c) line-item prices or total bid, proposal, or prequalification application prices. The classification of an entire proposal or of pricing as a trade secret or proprietary information is not acceptable and will not be honored by VCCS or the Commonwealth.

You should also provide as a separate appendix to your proposal a list of all pages in the proposal that contain proprietary information and the reason you deem the information proprietary.

Suppliers should keep in mind that procurement and contract records are generally public records open to inspection in accordance with the Virginia Freedom of Information Act (*see* Code § 2.2-4342(A)) and that transparency in procurement, contracting, and other governmental functions serves important public policy objectives. *See* Code §§ 2.2-4300(C) & 2.2-3700(B). Accordingly, Suppliers should not designate as trade secrets or proprietary information any more of their proposal than is necessary.

By submitting a proposal in response to the RFP, a Supplier grants VCCS a worldwide, royalty-free, non-sublicensable, non-exclusive, irrevocable license to retain, reproduce, and use the proposal (including any exhibits or other documents or materials the proposal incorporates) in any format for governmental purposes required or provided for by Virginia law. The foregoing includes, but is not limited to, the right for AGENCY to use information submitted in response to this document in any manner AGENCY may deem appropriate in evaluating the fitness of the services or solution(s) proposed

VI. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. GENERAL PROPOSAL PREPARATION

1. RFP Response: In order to be considered, offerors **must** submit a complete response to this RFP (electronic) through eVA, the Commonwealth's electronic procurement system no later than 5:00 p.m., Eastern time on May 9th, 2025. No other distribution of the proposal shall be made by the offeror. Offerors proposals will remain valid until contract award.

   a. Response:

      1) **One (1) original** proposal including the RFP, coversheet, and signed acknowledgement of any addenda (if applicable) ***Email is not acceptable.***
      2) **One (1) redacted copy** (only if offeror has invoked the protections trade of §2.2-4342F of the *Code of Virginia).* Redacted copy must be identical to the original copy with the exception of removal/overwritten redacted information – (marked "REDACTED"). ***Email is not acceptable.***

2. Proposal Preparation:

a. Ownership of all data, materials, and documentation originated and prepared for the VCCS pursuant to this solicitation shall belong exclusively to the VCCS and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act; however, the offeror must invoke the protections of § 2.2-4342F of the *Code of Virginia*, in writing, either before or at the time the data or other material 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 material 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 in the original submitted proposal. Additionally, the offeror must submit a redacted copy of the proposal if invoking said protection**. 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 of the proposal.

b. Proposals shall be submitted 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 submission 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.

c. Proposals should 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.

d. The entire proposal response should be **limited to 100 typed pages** (excluding the complete RFP, without attachments) submitted and filled out as required. No font shall be smaller than 11 Point. Page size shall be 8 ½ x 11 inch. Larger pages are allowed for figures or tables but should be used sparingly. All pages should be numbered. **eVA has a maximum file size per attachment of 60 MB.**

e. 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. Please 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 an 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.

f. 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's proposal.

3. Oral Presentation / Demonstrations/Site Visits: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation or provide a demonstration of their proposed solution to the agency. 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. The issuing agency will schedule the time and location of these presentations. Oral presentations are an option of the purchasing agency and may or may not be conducted. The College reserves the right to conduct an on-site inspection of the Offeror's facility in order to meet with personnel and evaluate facilities prior to contract award. This pre-award site visit will be provided at no cost to the Offeror.

B. **SPECIFIC PROPOSAL INSTRUCTIONS**

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

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

A. Offeror (Vendor) Data Sheet, included as an attachment to the RFP, all other attachments as noted, and other specific items or data requested in the RFP.

B. A written narrative statement to include:

1. **Business** – State your firm's core business, background, and experience in the relevant market, (Not to exceed 3 pages)

2. **Corporate Identity** – Provide the identity of any parent entity, including address, phone, and fax numbers, FEIN or Tax ID No., company website and contact email. Provide the identity of any of your subsidiaries, as applicable, (not to exceed 3 pages).

3. **Organization and Structure** - Please provide an overview of your firm's organizational operating structure and describe the operational and functional relationships of the business

units within your organization, as they relate to your proposal and VCCS's stated needs and requirements. Organizational charts are helpful supplements to the descriptions.

Indicate whether your firm expects to provide the Service's with existing resources or plans to secure additional resources by partnering or subcontracting. If applicable, identify the additional resources required to provide the Service's included in the proposal and the timetable for obtaining such resources. If your firm expects to utilize a partnership or subcontracting relationship, any such partner or subcontractor shall comply with the requirements of Section 2.F above.

4. **Strategic Relationships** - Please identify any and all strategic relationships with other related Suppliers you have or anticipate having. State all subcontractors expected to be employed and outsourced Service to be used in implementing the proposed solution. VCCS reserves the right to request that Supplier provide all the information described in this section for any and all major subcontractors proposed by Supplier.

5. **Financial Information**

   i. **Total Annual Revenue** – State your total annual revenue and indicate the revenues associated with the provision of services relevant to your proposal.

   ii. **Dun and Bradstreet Credit Report** – Include your firm's current full D&B business Report, if D&B issues reports on Offeror.

   iii. **Annual Reports** - Please provide certified, audited financial statements (i.e., income statements, balance sheets, cash flow statements) for the most recent three years. (Any Supplier that has been in business for a shorter period of time is requested to submit any available certified, audited annual financial statements.) VCCS may request copies of or access to current and historic annual reports. VCCS reserves the right to access a Supplier's publicly available financial information and to consider such information in its evaluation of such Supplier's proposal.

6. **Offeror Experience Level and Customer References** - You should have a demonstrable, proven record of providing Service similar to those defined in Section III to customers of similar scope and complexity. Please provide three customer references, with contact names, email addresses, phone numbers, Solution descriptions, and dates implemented that VCCS may use as a reference check in evaluating your proposal. VCCS will make such reasonable investigations as deemed proper and necessary to determine the ability of a Offeror to perform a resultant contract. These may include, but may not be limited to, reference checks and interviews. The references should be from organizations where Offeror is providing Services that are similar in type and scope to those identified in Section III.

7. **Security Risk Management Overview** - Provide an overview of your firm's comprehensive security risk management processes including your application, monitoring, and

management of the controls used. Provide details as to how you establish the context for security risk-based decisions, how you assess the risk, how you respond to the risk once it's determined, and how you monitor the risk on an ongoing basis using communications and feedback for continuous improvement within your organization.

8. **Account Management Plan** - Provide a detailed description of the approach that your firm would take in order to manage the business and performance aspects of an awarded contract. Provide a detailed description of the approach your firm would take to support self-sufficiency of a public body with respect to the solution and the transition of solution management to a public body requesting such transition.

C. Specific methodology and plans for providing the proposed services including:
   1. What, when, how and by whom the services will be performed or accomplished.
   2. Projected timeline for delivery of services relative to award date of contract.
   3. Implementation of system
   4. Experience of Offeror and personnel
   5. Project Management requirements

D. Proposed fees: Complete Attachment 6 – Pricing Schedule for all goods and services as outlined in this RFP.

VII. EVALUATION AND AWARD CRITERIA

A. EVALUATION CRITERIA: Proposals will be evaluated by the VCCS using the following criteria:

Evaluation Criteria	% of Total
Specific Plan, Implementation, and Scaling	20
Experience and Qualifications	15
Technical Requirements (Security, AI, and Compliance)	30
Maintenance and Support	15
Proposed Pricing	10
Small Business Plan	10
TOTAL	**100**

B. AWARD: 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 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 (Code of Virginia, § 2.2-4359D). 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.

VIII. GENERAL TERMS AND CONDITIONS

A. **ANTI-DISCRIMINATION:** By submitting their bids, bidders 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 § 2.2-4311 of the *Virginia Public Procurement Act (VPPA).* 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. (*Code of Virginia*, § 2.2-4343.1E).

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 the requirements of this section.

d. If the contractor employs more than five employees, the contractor shall (i) provide annual training on the contractor's sexual harassment policy to all supervisors and employees providing services in the Commonwealth, except such supervisors or employees that are required to complete sexual harassment training provided by the Department of Human Resource Management, and (ii) post the contractor's sexual harassment policy in (a) a conspicuous public place in each building located in the Commonwealth that the contractor owns or leases for business purposes and (b) the contractor's employee handbook.

e. The requirements of these provisions 1. and 2. are a material part of the contract. If the Contractor violates one of these provisions, the Commonwealth may terminate the affected part of this contract

for breach, or at its option, the whole contract. Violation of one of these provisions may also result in debarment from State contracting regardless of whether the specific contract is terminated.

f. In accordance with Executive Order 61 (2017), a prohibition on discrimination by the contractor, in its employment practices, subcontracting practices, and delivery of goods or services, on the basis of race, sex, color, national origin, religion, sexual orientation, gender identity, age, political affiliation, disability, or veteran status, is hereby incorporated in this contract.

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.

B. **ETHICS IN PUBLIC CONTRACTING:** By submitting their bids, bidders certify that their bids are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other bidder, supplier, manufacturer or subcontractor in connection with their bid, 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.

C. **IMMIGRATION REFORM AND CONTROL ACT OF 1986:** Applicable for all contracts over $10,000: 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.

D. **DEBARMENT STATUS:** By participating in this procurement, the vendor certifies that they are not currently debarred by the Commonwealth of Virginia from submitting a response for the type of goods and/or services covered by this solicitation. Vendor further certifies that they are not debarred from filling any order or accepting any resulting order, or that they are not an agent of any person or entity that is currently debarred by the Commonwealth of Virginia.

If a vendor is created or used for the purpose of circumventing a debarment decision against another vendor, the non-debarred vendor will be debarred for the same time period as the debarred vendor.

E. **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.

F. **MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS FOR RFPs: Failure** to submit a proposal on the official state form provided for that purpose shall be a cause for rejection of the proposal. Modification of or additions to any portion of the Invitation for Offeror's 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 as nonresponsive. As a precondition to its acceptance, the Commonwealth may, in its sole discretion, request that the bidder withdraw or modify nonresponsive portions of a bid which do not affect quality, quantity, price, or delivery. No modification of or addition to the provisions of the contract shall be effective unless reduced to writing and signed by the parties.

G. **CLARIFICATION OF TERMS:** If any prospective bidder has questions about the specifications or other solicitation documents, the prospective bidder 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.

H. **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 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 resolved in accordance with *Code of Virginia,* § 2.2-4363 and -4364. Upon determining that invoiced charges are not reasonable, the Commonwealth shall notify the contractor of defects or improprieties in invoices within fifteen (15) days as required in *Code of Virginia,* § 2.2-4351. 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 (*Code of Virginia,* § 2.2-4363).

2. To Subcontractors:

   a. Within seven (7) days of the contractor's receipt of payment from the Commonwealth, a contractor awarded a contract under this solicitation is hereby obligated:

      (1) To pay the subcontractor(s) 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 subcontractor(s), 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.

I. **PRECEDENCE OF TERMS:** The following General Terms and Conditions, Information Security Standard – Public Cloud Services, IT Terms and Conditions, Special Terms and Conditions, APPLICABLE LAWS AND COURTS, ANTI-DISCRIMINATION, ETHICS IN PUBLIC CONTRACTING, IMMIGRATION REFORM AND CONTROL ACT OF 1986, DEBARMENT STATUS, ANTITRUST, MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS, CLARIFICATION OF TERMS, PAYMENT 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.

J. **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.

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

L. **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 terms, conditions, or scope of the contract. Any additional goods or services to be provided shall be of a sort that is ancillary to the contract goods or services, or within the same broad product or service categories as were included in the contract award. Any 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, unless the contractor intends to claim an adjustment to compensation, schedule, or other contractual impact that would be caused by complying with such notice, in which case the contractor shall, in writing, promptly notify the Purchasing Agency of the adjustment to be sought, and before proceeding to comply with the notice, shall await the

Purchasing Agency's written decision affirming, modifying, or revoking the prior written notice. If the Purchasing Agency decides to issue a notice that requires an adjustment to compensation, 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 dispute's provisions of the Commonwealth of Virginia *Vendors Manual*. 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.

M. **DEFAULT:** In case of failure to deliver goods or services in accordance with the contract terms and conditions, the Commonwealth may terminate this agreement after verbal or written notice without penalty. Upon termination the Commonwealth may procure the goods and services contracted for 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.

N. **TAXES:** Sales to the Commonwealth of Virginia are normally exempt from State sales tax. State sales and use tax certificates of exemption, Form ST-12, will be issued upon request. Deliveries against this contract shall usually be free of Federal excise and transportation taxes. The Commonwealth's excise tax exemption registration number is 54-73-0076K.

If sales or deliveries against the contract are not exempt, the contractor shall be responsible for the payment of such taxes unless the tax law specifically imposes the tax upon the buying entity and prohibits the contractor from offering a tax-included price.

O. **INDEMNIFICATION**

A. Indemnification Generally

Supplier shall defend, indemnify, and hold harmless all Commonwealth Indemnified Parties from and against any third-party Claims to the extent the Claims in any way relate to, arise out of, or result from:

i. Any negligent act, negligent omission, or intentional or willful conduct of Supplier or any Supplier Personnel.

ii. A breach of any representation, warranty, covenant, or obligation of Supplier contained in this contract.

iii. Any defect in the Supplier-provider products or services.

iv. Any actual or alleged infringement or misappropriation of any third party's intellectual property rights by any of the Supplier-provider products or services: or

v. Any Claims by any Subcontractor resulting from Supplier's failure to pay such Subcontractor.

B. Defense Claims

Supplier will be solely responsible for all costs and expenses associated with the defense of all third-party Claims against Commonwealth Indemnified Parties. Selection and approval of counsel, and approval of any settlement, shall be accomplished in accordance with all applicable laws, rules, and regulations. For state agencies, the applicable laws include §§ 2.2-507, 2.2-510 and 2.2-514 of the Code.

C. Duty to Replace or Reimburse

In the event of a Claim pursuant to any actual or alleged infringement or misappropriation of any third party's intellectual property rights by any of the Supplier-provided products or services, or Supplier's performance, Supplier shall, at its expense and option, either (a) procure the right to continue use of such infringing products or services, or any components thereof, or (b) replace or modify the infringing products or services or any components thereof, with non-infringing products or services satisfactory to VCCS.

In the event that Agency cannot use the affected Deliverable, Product, Licensed Services, or Services, including any Components, then Supplier shall reimburse such Agency for the reasonable cost incurred by such Agency in obtaining an alternative product or service.

D. Supplier Dispute of Obligation to Indemnify

If a Claim is commenced against any Commonwealth indemnified Parties by a third party alleging an infringement of the third party's intellectual property rights and Supplier is of the opinion that the allegations in the third party's Claim, in whole or in part, are not covered by the indemnification provision in this Contract, the Supplier shall immediately notify Agency and the affected Agency(s) in writing and shall, nonetheless, take all reasonable steps to protect the rights, remedies, and interests of the Commonwealth Indemnified Parties in the defense of the claim, including to secure a continuance to permit Agency and the affected Agency(s) to appear and defend their interests in cooperation with Supplier as is appropriate, including any jurisdictional defenses Agency or the effected Agency(s) may have.

P. **LIABILITY**

A. Supplier Liability

Supplier agrees that it is fully responsible for all acts and omissions of Supplier Personnel, including their negligence, gross negligence, or willful misconduct, under this contract.

The supplier's liability and indemnification obligations under this contract shall not exceed, in aggregate, twice the value of the contract, during the contract term. For purposes of this contract, "value of the contract" means the cumulative spend under this contract – including any orders, SOW's, or Change Orders thereto-by the Commonwealth.

The limitations of liability set forth in this section will not apply to liability arising from any combination of the following:

i. Any intentional or willful misconduct, fraud, or recklessness of Supplier or any Supplier Personnel; or

ii. Claims for bodily injury, including death, and damage to real property or tangible property resulting from the negligence of a Supplier or any Supplier Personnel.

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 §§ 2.2-4332 and 65.2-800 et seq. of the *Code of Virginia*. The offeror further certifies that the contractor and any subcontractors will maintain this 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. Offeror shall provide evidence of insurance and access to a copy of Offeror's policy documents upon request by VCCS.

MINIMUM INSURANCE COVERAGES AND LIMITS:

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 requirements under the *Code of Virginia* during the course of the contract shall be in noncompliance with the contract.

2. Errors and omission - $5,000,000 per occurrence

3. Cyber Security Liability - $5,000,000 per occurrence

4. Employer's Liability - $100,000.

5. 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 shall be added as an additional insured to the policy by an endorsement.

6. 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 as a result of this solicitation, the purchasing agency will publicly post such notice on the DGS/DPS eVA VBO (www.eva.virginia.gov) for a minimum of 10 days.

S. **DRUG-FREE WORKPLACE:** Applicable for all contracts over $10,000:

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**: A bidder 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 bidder or 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, web site 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 e-procurement solution by completing the free eVA Vendor Registration. All bidders must register in eVA and pay the Vendor Transaction Fees specified below; failure to register will result in the bid being rejected.

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

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

        i. DSBSD-certified Small Businesses: 1%, capped at $500 per order.
        ii. Businesses that are not DSBSD-certified Small Businesses: 1%, capped at $1,500 per order.

b. Refer to Special Term and Condition "eVA Orders and Contracts" to identify the number of purchase orders that will be issued as a result of this solicitation/contract with the eVA transaction fee specified above assessed for each order.

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

The specified vendor transaction fee will be invoiced, by the Commonwealth of Virginia Community College System Department of General Services, typically within 60 days of the order issue 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 agency shall be bound hereunder only to the extent that the legislature has appropriated funds that are legally available or may hereafter become legally available for the purpose of this agreement.

W. **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 pursuant to the *Virginia Public Procurement Act* 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.

X. **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 agency training on civility in the State workplace if contractor's (and any subcontractor's) regular mandatory training programs do not already encompass equivalent or greater expectations. 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.

Y. GOVERNING LAW: This Contract is governed by and will be construed in accordance with the laws of the Commonwealth of Virginia without regard to that body of law controlling choice of law. Any and all litigation relating to this Contract must be brought in the circuit courts of the Commonwealth of Virginia. The English language version of this Contract prevails when interpreting this Contract. The United Nations Convention on Contracts for the International Sale of Goods and all other laws and international treaties or conventions relating to the sale of goods are expressly disclaimed. The Uniform Computer Information Transactions Act applies to this Contract only to the extent required by Code § 59.1-501.15.

Z. MODIFICATIONS: This Contract may be modified in accordance with § 2.2-4309 of the Code of Virginia. Such modifications may only be made by the representatives authorized to do so. No modifications to this Contract shall be effective unless it is in writing and signed by the duly authorized representative of both parties. No term or provision hereof shall be deemed waived, and no breach excused unless such waiver or consent to breach is in writing.

Any contract issued on a firm fixed price basis may not be increased more than twenty five percent (25%) or $50,000.00, whichever is greater, without the approval of the Governor of the Commonwealth of Virginia or his authorized designee. In no event may the amount of the Contract be increased without adequate consideration.

The provisions of this section shall not limit the amount a party to a public contract may claim or recover against a public body pursuant to § 2.2-4363 (contractual claims) or any other applicable statute or regulation. The unauthorized approval of a modification cannot be the basis of a contractual claim as set forth in § 2.2-4363.

AA. SEXUAL HARASSMENT TRAINING: Pursuant to requirements of § 2.2-4201(3) for any Contract over $10,000, Supplier agrees that it shall (i) provide annual training on the Supplier's sexual harassment policy to all supervisors and employees providing services in the Commonwealth of Virginia, except such supervisors or employees that are required to complete sexual harassment training provided by the Virginia Department of Human Resource Management, and (ii) post the contractor's sexual harassment policy in (a) a conspicuous public place in each building located in the Commonwealth of Virginia that the Supplier owns or leases for business purposes and (b) the Supplier's employee handbook.

Additionally, Supplier shall include these provisions in every subcontract or purchase order of over $10,000, so that such provisions shall be binding upon each subcontractor or vendor.

BB. SECTION 508 COMPLIANCE: All information technology which, pursuant to this Contract, 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 Supplier must provide a detailed explanation of how compliance with Section 508 of the Rehabilitation Act is achieved and a validation of concept demonstration. 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.

CC. NON-VISUAL ACCESS: All information technology (the "Technology") which is purchased or upgraded by the VCCS will comply with the following non-visual access standards from the date of purchase or upgrade until the expiration of this Agreement:

- Effective, interactive control and use of the Technology will be readily achievable by non-visual means;
- Technology equipped for non-visual access will be compatible with information technology used by other individuals with whom any blind or visually impaired user of the Technology interacts;
- Non-visual access technology will be integrated into any networks used to share communications among employees, program participants or the public; and
- Technology for non-visual access will have the capability of providing equivalent access by non-visual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

Compliance with the foregoing non-visual access standards will not be required if the Director of Strategic Sourcing, VCCS of Virginia determines that 1) the Technology is not available with non-visual access because the essential elements of the Technology are visual and 2) non-visual equivalence is not available.

Installation of hardware, software, or peripheral devices used for non-visual 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 will permit the installation and effective use of non-visual access software and peripheral devices.

If requested, this Contract must provide a detailed explanation of how compliance with the foregoing non-visual access standards is achieved and a validation of concept demonstration.

DD. CONTRACT EXTENSIONS: In the event that the original term and all renewals of this contract expire prior to the award for a new contract for similar goods and/or services, the Commonwealth of Virginia may, with written consent of the Contractor, extend this contract for such a period as may be necessary to afford the Commonwealth of Virginia a continuous supply of the identified goods and/or services.

EE. APPLICABLE LAWS AND COURTS: This solicitation and any resulting contract shall be governed in all respects by the laws of the Commonwealth of Virginia, without regard to its choice of law provisions, and any litigation with respect thereto shall be brought in the circuit courts of the Commonwealth. The agency and the contractor are encouraged to resolve any issues in controversy arising from the award of the contract or any contractual dispute using Alternative Dispute Resolution (ADR) procedures (Code of Virginia, § 2.2-4366). ADR procedures are described in Chapter 9 of the Vendors Manual. The contractor shall comply with all applicable federal, state, and local laws, rules and regulations.

IX. SPECIAL TERMS AND CONDITIONS

A. **AUDIT:** The contractor shall retain all books, records, 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 agency, 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. **TERM AND TERMINATION:**

1. Contract Term: This Contract is effective and legally binding as of the Effective Date and, unless terminated as provided for in this section, will be effective and legally binding for a period of two (2) years ("Initial Term"). VCCS, in its sole discretion, may renew this Contract for up to four (4) additional two (2) year renewal periods after the expiration of the Initial Term (collectively with the Initial Term, the "Contract Term"). VCCS will issue a written notification to the Supplier stating VCCS's intention to exercise a renewal period no less than 30 calendar days prior to the expiration of any current term. In addition, performance of an order or SOW issued during the Contract Term may survive the expiration of the Contract Term, in which case all contractual terms and conditions required for the operation of such order or SOW will remain in full force and effect until all of Supplier's obligations pursuant to such order or SOW have met the final Acceptance criteria of VCCS.

2. Termination for Convenience: VCCS may terminate this Contract, in whole or in part, at any time and for any reason upon not less than 30 calendar days prior written notice to Supplier. VCCS may terminate an order or SOW, in whole or in part, at any time and for any reason upon not less than 30 calendar days prior written notice to Supplier. Any termination under this provision will not affect the rights and obligations attending any order or SOW outstanding at the termination date.

3. Termination for Breach: In the event of breach by the Supplier, VCCS will have the right to terminate this Contract, in whole or in part, and VCCS may terminate an order or SOW issued hereunder, in whole or in part. Supplier will be deemed in breach in the event that Supplier fails to meet any material obligation set forth in this Contract or in any order or SOW issued hereunder. Any termination under the provisions of this section will be deemed a "Termination for Breach".

   If VCCS deems the Supplier to be in breach, VCCS shall provide Supplier with notice of breach and allow Supplier 15 business days to cure the breach. If Supplier fails to cure the breach as noted, VCCS may immediately terminate this Contract or any order or SOW issued pursuant to this Contract, in whole or in part.

   If VCCS deems the Supplier to be in breach of an order or SOW, that VCCS shall provide Supplier with notice of breach and allow Supplier 15 business days to cure the breach. If Supplier fails to cure the breach as noted, VCCS may immediately terminate its order or SOW, in whole or in part. In addition, if Supplier is found by a court of competent jurisdiction to be in violation of or to have violated 31 U.S.C. § 1352, or if Supplier becomes a party excluded from Federal Procurement and Non-procurement Programs, VCCS may immediately terminate this Contract, in whole or in part, for breach, and VCCS shall provide written notice to Supplier of such termination. Supplier shall provide prompt written notice to VCCS if Supplier is charged with violation of 31 U.S.C. § 1352, or if federal debarment proceedings are instituted against Supplier.

4. Termination for Non-Appropriation of Funds: All payment obligations from public bodies under this Contract are subject to the availability of legislative appropriations at the federal, state, or local level for this purpose. In the event of non-appropriation of funds, irrespective of the source of funds, for the items under this Contract, VCCS may terminate this Contract, in whole or in part, or any order or SOW, in whole or in part, or VCCS may terminate an order or SOW, in whole or in part,

for those goods or services for which funds have not been appropriated. Written notice will be provided to the Supplier as soon as possible after legislative action is completed.

5. Effect of Termination: Upon termination, neither the Commonwealth, nor VCCS will have any future liability except for Deliverables accepted by VCCS or Services (including any applicable Licensed Services and Maintenance Services) rendered by Supplier and accepted by VCCS prior to the termination date.

   In the event of a Termination for Breach, Supplier shall accept return of any Deliverable that was not accepted by VCCS, and Supplier shall refund any monies paid by any VCCS for the unaccepted Deliverable. VCCS will also have the right, in its sole discretion, to return any accepted Deliverable and Supplier shall refund any monies paid for the accepted Deliverable, less a reasonable value for the use of those components. Supplier will bear all costs of de-installation and return of Deliverables.

6. Termination by Supplier: In no instance will termination by Supplier be considered. Failure by VCCS to make timely payments owed to Supplier for its performance under this Contract will constitute a breach by that VCCS. Supplier's remedy for a breach is limited to the remedies set forth in Code § 2.2-4363 and the "Remedies" section of this Contract below.

7. Transition of Services: At the request of VCCS prior to or upon expiration or termination of this Contract, Supplier shall provide all assistance as VCCS may reasonably require to transition the Supplier's contractual obligations, or any portion thereof, to any other supplier with whom VCCS contracts for provision of same. This Transition Period obligation may extend beyond expiration or termination of the Contract for a period of six months. If this Contract includes Supplier's provision of licensed products, Supplier shall take no action to restrict or terminate the use of such licensed products after the date of expiration or termination of the Contract or during any Transition Period, or both. VCCS shall pay for any additional maintenance or licensing fees during any Transition Period at the hourly rate or at a fee agreed upon by Supplier and VCCS. Supplier shall provide all reasonable transition assistance requested by VCCS to allow for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to VCCS. The transition assistance will be deemed by the parties to be governed by the terms and conditions of this Contract, except for those terms or conditions that do not reasonably apply to transition assistance. Further, any Transition Period will not affect any VCCS's rights in regards to any purchased Software perpetual licenses which are paid in full.

C. **RENEWAL OF CONTRACT:** This contract may be renewed by the Commonwealth for up to four (4) successive (2) two-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 two-year period, the contract price(s) for the additional three years shall not exceed the contract price(s) of the original contract increased/decreased by more than the percentage increase/decrease of the

services category of the CPI-U 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 services category of the CPI-U section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

D. **eVA ORDERS AND CONTRACTS:** The solicitation/contract will result in **multiple** purchase orders with the applicable eVA transaction fee assessed for each order.

Vendors desiring to provide goods and/or services to the Commonwealth shall participate in the eVA Internet e-procurement solution and agree to comply with the following: If this solicitation is for a term contract, failure to provide an electronic catalog (price list) or index page catalog for items awarded will be just cause for the Commonwealth to reject your bid or terminate the contract for default. The format of this electronic catalog shall conform to the eVA Catalog Interchange Format (CIF) Specification that can be accessed and downloaded from www.eVA.virginia.gov. Contractors should email Catalog or Index Page information to eVA-catalog-manager@dgs.virginia.gov.

E. **FINAL INSPECTION:** At the conclusion of the work, the contractor shall demonstrate to the authorized owner's representative that the work is fully operational and in compliance with contract specifications and codes. Any deficiencies shall be promptly and permanently corrected by the contractor at the contractor's sole expense prior to final acceptance of the work.

F. **SUBMISSION OF SMALL BUSINESS SUBCONTRACTING PLAN, EVIDENCE OF COMPLIANCE WITH SMALL BUSINESS SUBCONTRACTING PLAN, AND SUBCONTRACTOR REPORTING:**

1. Submission of Small Business Subcontracting Plan: It is the statewide goal of the Commonwealth that 42% of its purchases be made from small businesses certified by DSBDS. This includes discretionary spending in prime contracts and subcontracts. All bidders are required to submit a Small Business Subcontracting Plan. The contractor is encouraged to offer such subcontracting opportunities to DSBDS-certified small businesses. This shall include DSBDS-certified woman-owned and minority-owned businesses and businesses with DSBDS service-disabled veteran-owned status when they have also received DSBSD small business certification. Where it is not practicable for any portion of the goods/services to be subcontracted to other supplies, the bidder shall note such on the Small Business Subcontracting Plan. No bidder or subcontractor shall be considered a small business unless certified as such by the Department of Small Business and Supplier Diversity (DSBSD) by the due date for receipt of bids.

2. Evidence of Compliance with Small Business Subcontracting Plan**:** 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 timely reports substantiating compliance in accordance with the small business subcontracting plan. If a variance exists, the contractor shall provide a written explanation. A subcontractor shall be considered a Small Business for purposes of a contract if and only if the subcontractor holds a certification as such by the DSBSD. Payment(s)

may be withheld until the purchasing agency confirms that the contractor has certified compliance with the contractor's submitted Small Business Subcontracting Plan or is in receipt of a written explanation of the variance. The agency or institution reserves the right to pursue other appropriate remedies for non-compliance to include, but not be limited to, termination for default.

3. Prime Contractor Subcontractor Reporting:

i. Each prime contractor who wins an award greater than $100,000 shall deliver to the contracting agency or institution on a quarterly basis, information on use of subcontractors that are DSBSD-certified businesses or ESOs. The contractor agrees to furnish the purchasing office at a minimum the following information: name of firm, phone number, total dollar amount subcontracted, category type (Businesses that are DSBSD-certified small, women-owned, minority-owned, Service-Disabled Veteran, or Employment Services Organization) and type of product provided at the frequency required.

ii. In addition, each prime contractor who wins an award greater than $200,000 shall deliver to the contracting agency or institution on a quarterly basis, information on use of subcontractors that are **not** DSBSD-certified businesses. The contractor agrees to furnish the purchasing office at a minimum the following information: name of firm, phone number, total dollar amount subcontracted, and type of product/service provided, at the frequency required.

G. **CONTINUITY OF SERVICES**:

1. The Contractor recognizes that the services under this contract are vital to the Agency and must be continued without interruption and that, upon contract expiration, a successor, either the Agency or another Contractor, may continue them. The contractor agrees:

i. To exercise its best efforts and cooperation to affect an orderly and efficient transition to a successor.

ii. To make all Agency owned facilities, equipment, and data available to any successor at an appropriate time prior to the expiration of the contract to facilitate transition to successor; and

iii. That the Agency Contracting Officer shall have final authority to resolve disputes related to the transition of the contract from the Contractor to its successor.

2. The contractor shall, upon written notice from the Contract Officer, furnish phase-in/phase-out services for up to One Hundred and eighty (180) days after the contract expires and shall negotiate in good faith a plan with the successor to execute the phase-in/phase-out services. This plan shall be subject to the Contract Officer's approval.

3. The Contractor shall, be reimbursed for all reasonable, pre-approved phase-in/phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under the contract. All phase-in/phase-out work fees must be approved by the Contract Officer in writing prior to commencement of said work.

H. **SPECIAL EDUCATIONAL OR PROMOTIONAL DISCOUNTS**: The contractor shall extend any special educational or promotional sale prices or discounts immediately to the Commonwealth during the term of the contract. Such notice shall also advise the duration of the specific sale or discount price.

I. **E-VERIFY PROGRAM: EFFECTIVE** 12/1/13. Pursuant to *Code of Virginia*, §2.2-4308.2, 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 any agency of the Commonwealth 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 such public contract. Any such employer who fails to comply with these provisions shall be debarred from contracting with any agency of the Commonwealth for a period up to one year. Such debarment shall cease upon the employer's registration and participation in the E-Verify program. If requested, the employer shall present a copy of their Maintain Company page from E-Verify to prove that they are enrolled in E-Verify.

J. **ENVIRONMENTAL COMPLIANCE REQUIREMENTS:** The contractor must comply with all Environmental Compliance Requirements covered in the Northern Virginia Community College Good Housekeeping and Pollution Prevention Manual (https://www.nvcc.edu/stormwater/_docs/NOVA-Good-Housekeeping-and-Pollution-Prevention-Manual.pdf).

K. **LIABILITY FOR MISUSE:** The Offeror/Bidder agrees to indemnify and hold harmless the Commonwealth of Virginia, its agencies, including without limitation Virginia Community College System, their respective officers, and employees from any claims, damages, or liabilities arising from the misuse of Artificial Intelligence (AI) technologies in the proposal development process.

L. **ISSUE NOTIFICATION:** If either party detects any AI-related issues, including data breaches, inaccurate, biased, or unrepresentative outputs, they must promptly notify the other party within 24 hours, providing a detailed description and immediate mitigation steps. Both parties will collaborate on a remediation plan, with the customer having the right to suspend AI use until the issue is resolved. If unresolved within 30 days, the customer may terminate the agreement without penalty. Both parties agree to act diligently and bear their own costs for issue resolution.

M. **VCCS AUTHORIZED USERS**: This solicitation is being conducted on behalf of the Virginia Community College System (VCCS) including its twenty-three (23) Community Colleges, the Virginia Community College System Office and the Shared Services Center (SSC). Any of the VCCS colleges and/or the System Office and/or the SSC may utilize any contract(s) awarded as a result of this solicitation. A list of VCCS colleges is available on-line at www.vccs.edu.

X. IT TERMS AND CONDITIONS

A. **CONTENT PRIVACY AND SECURITY**: Contractor shall provide a secure environment for Content and any hardware and software, including servers, network and data components provided by Contractor as part of its performance under this Contract. Contractor shall provide a secure environment for Content and any hardware and software in accordance with the VCCS Security Standard Public Cloud Services attached to this contract in order to prevent unauthorized access to and use or modification of, and to protect, the Application and Content. Contractor agrees that all Content of the Agency is intended solely for the

business of the agency and is considered private data. Therefore, Contractor shall, at a minimum, implement the following procedures designed to protect the privacy and security of Content:

I. User identification and access controls designed to limit access to Content to Application Users.

II. External connections to the World Wide Web which will have appropriate security controls including industry standard intrusion detection and countermeasures that will detect and terminate any unauthorized activity prior to entering the firewall maintained by Contractor.

III. Industry standard firewalls regulating all data entering Contractor's internal data network from any external source which will enforce secure connections between internal and external systems and will permit only specific types of data to pass through.

IV. Industry standard encryption techniques which will be used when Content is processed, transmitted, or stored by Contractor on behalf of the agency.

V. Physical security measures, including securing all Content on a secure server, in locked data cabinets within a secure facility located within the Continental United States. Access to facilities housing the Application and Content restricted to only allow access to personnel and agents of Contractor who have a need to know in connection with operation and support of the Application.

VI. A backup of Content, for an orderly and timely recovery of such data in the event that the Licensed Services may be interrupted. Unless otherwise described in a Statement of Work, Service Provider shall maintain a backup of Content that can be recovered as per the stated Service Levels. Additionally, Service Provider shall store a backup of Customer Data in an off-site "hardened" facility, located within the United States no less than daily, maintaining the security of Customer Data, the security requirements of which are further described herein.

VII. Contractor agrees to maintain and follow a disaster recovery plan designed to maintain Application User access to the Application and Licensed Services, and to prevent the unintended destruction or loss of Content; and which plan, unless otherwise specified herein, shall provide for daily back-up of Content and archival of such Content at a secure facility located within the United States. The disaster recovery plan shall provide for and be followed by Contractor such that in no event shall the Application, Licensed Services, Contractor Product and/or Content be unavailable to any Application User for a period in excess of seventy-two (72) hours.

VIII. Contractor agrees that during the term of this Contract, Contractor will retain the agency's Content for the full term of the Contract.

IX. Contractor, its employees, agents, and Subcontractors, shall immediately notify the agency, of any degradation, potential breach or breach of Content and Application privacy or security in any systems supporting the Licensed Services. Contractor shall provide the agency the opportunity to participate in the investigation of the reported situation and to exercise control over reporting the unauthorized disclosure, to the extent permitted by law.

X. Contractor shall be required to notify the agency in writing thirty (30) days prior to its intention to replace or add any third-party that will be provided access to Content whether that access is provided by Contractor or Contractor's Subcontractors. The agency may reject any additional or new third parties who may be provided access to Content.

XI. Contractor shall, at all times, remain compliant with the privacy and security requirements mandated by federal, state, and local laws and regulations.

XII. Contractor shall ensure performance of a SOC2 Type II audit (or equivalent) at least once annually of Contractor's environment inclusive of the contractor's own software development, management, and remote access or administration by contractor personnel. Upon request from the agency (not more than once annually), Contractor shall provide the agency with a copy of Contractor's final SOC2 Type II audit report. Contractor shall also assist VCCS in obtaining the current SOC2 Type II audit report from any third-party providing services to Contractor, if said third-party services involve the processing or storage of Participating VCCS Content.

XIII. Contractor's failure to comply with the provisions in items (I) through (XII) shall constitute a breach of this Contract.

XIV. Within fifteen (15) business days after the expiration or termination of this Contract, Contractor shall confirm in writing to the agency that all Content has been removed from all systems where the Content resided during performance of this Contract in a manner that complies with and/or exceeds the Commonwealth Data Removal standard located at the then-current data removal standard: ITRM standard SEC 514-04 https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/SEC514_05.01-Removal-COV-Data-from-Electronic-Media-Standard.pdf. The written confirmation shall include (i) sufficient detail describing the processes and procedures used in removing the Content, (ii) information about the locations of where it was removed from within the Application and storage and other locations, and (ii) the date the removals were performed. All metadata, in its original form, shall be returned to the respective Participating Agency(s).

XV. Any Participating Agency of this Contract agrees to notify Contractor of any degradation, potential breach, or breach of the Content and Application privacy or security as soon as possible after discovery. Any Participating Agency further agrees to provide Contractor the opportunity to participate in the investigation of the reported situation.

XVI. Regular training for Contractor personnel regarding the security and data recovery programs referenced in this Section.

XVII. Regular testing of the systems and procedures outlined in this Section; and

XVIII. Audit controls that record and monitor Application and Licensed Services activity continuously.

XIX. Contractor agrees to provide written notice within 24 hours to VCCS of all incidents that threaten or could potentially threaten the security of VCCS's Content and/or VCCS's use of the Licensed Services. This notice is required to allow the Agency to commence any necessary internal actions to remediate such incident, which may include a temporary suspension of use of the Licensed Service by Agency. If a suspension of use becomes necessary, the Supplier further agrees not to impose any penalty on VCCS, VCCS employees, or the Commonwealth.

B. **SECURITY COMPLIANCE**

I. Contractor agrees to comply with all provisions of the VCCS Information Security Standard Public Cloud Services Attachment 7. Contractor further agrees to comply with all provisions of VCCS then-current security procedures as are pertinent to Contractor's operation, and which have been or will be supplied to Contractor during the negotiation phase prior to the award of contract. Contractor shall also comply with all applicable federal, state, and local laws and regulations. For any individual agency location, security procedures may include but not be limited to background checks, records verification, photographing, and fingerprinting of Contractor's employees or agents. Contractor may, at any time, be required to execute and complete, for each individual Contractor employee or agent, additional forms which may include non-disclosure agreements to be signed by Contractor's employees or agents acknowledging that all agency information with which such employees and agents come into contact while at the agency site is confidential and proprietary. Any unauthorized release of proprietary or personal information by the Contractor or an employee or agent of Contractor shall constitute a breach of its obligations under this Section and the Contract.

II. Contractor shall immediately notify the VCCS of any Breach of Unencrypted and Unredacted Personal Information, as those terms are defined in Virginia Code 18.2- 186.6, and other personal identifying information, such as insurance data or date of birth, provided by the agency to Contractor. Contractor shall provide the agency the opportunity to participate in the investigation of the Breach and to exercise control over reporting the unauthorized disclosure, to the extent permitted by law.

III. Contractor shall indemnify, defend, and hold the Commonwealth, VCCS, their officers, directors, employees, and agents harmless from and against any and all fines, penalties (whether criminal or civil), judgments, damages, and assessments, including reasonable expenses suffered by, accrued against, or charged to or recoverable from the Commonwealth, Agency, their officers, directors, agents or employees, on account of the failure of Contractor to perform its obligations pursuant this Section.

IV. Agency shall have the right to review Contractor's information security program prior to the commencement of Licensed Services and from time to time during the term of any resulting contract or agreement. During the performance of the Licensed Services, on an ongoing basis from time to time, Agency shall be entitled to perform, or to have performed, an on-site audit of Contractor's information security program. In lieu of an on-site audit, upon request by Agency, Contractor agrees to complete, within forty-five (45 days) of receipt, an audit questionnaire

provided by Agency regarding Contractor's information security program. Contractor shall implement any reasonably required safeguards as identified by any program audit.

C. **GENERAL WARRANTY:** Contractor warrants and represents to the agency the Licensed Services and the Application described as follows:

I. Ownership: Contractor has the right to provide the Licensed Services, including access by the agency and its application users, without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party.

II. Licensed Services, Application, and Documentation: Contractor warrants the following with respect to the Licensed Services and the Application:

i. Contractor represents and warrants (i) that it shall perform the Licensed Services in conformity to the specifications set forth in a professional and workmanlike manner and (ii) that the Licensed Services shall not infringe any third-party proprietary rights including (without limitation) any trademark, trade name, trade secret, copyright, moral rights, patents, or similar intellectual property rights.

ii. Contractor warrants that the Application and Licensed Services will conform in all material respects to the requirements set forth in this solicitation, any resulting contract, purchase order, or scope of work issued hereunder. Contractor warrants that the Application Licensed Services will conform to the applicable specifications and documentation, not including any post-acceptance modifications or alterations to the documentation which represent a material diminishment of the functionality of the Application, Licensed Services, or contractor product. Contractor also warrants that such Application and Licensed Services are compatible with and will operate successfully when used on the equipment in accordance with the documentation and all of the terms and conditions hereof.

iii. The Application provided hereunder is at the current release level unless the agency specifies an older version in its order.

iv. No corrections, workarounds or future Application releases provided by Contractor shall degrade the Application, cause any other warranty to be breached, or require the agency to acquire additional hardware equipment or software.

v. Contractor warrants that all post-acceptance updates, changes, alterations or modifications to the Application, Licensed Services and documentation by Contractor will be compatible with and will not materially diminish the features or functionality of the Application, Licensed Services and/or contractor product when used on the equipment in accordance with the documentation and all of the terms and conditions hereof.

vi. Contractor warrants that the documentation and all modifications or amendments thereto which Contractor is required to provide under any resulting contract shall be sufficient in

detail and content to allow a user to understand and utilize fully the Application without reference to any other materials or information.

D. **DATA USE AND OWNERSHIP:** VCCS data remains the property of the VCCS, college, or organization for which the data was created. VCCS data may not be used for any purpose other than that for which it was collected except when used in aggregate by the VCCS or other authorized entity without personally identifiable information. At the end of any contract period or in the event of termination of the contract or agreement by either party the contractor shall transfer all data back to the VCCS in machine readable or other agreed to format. The contractor shall destroy all remaining copies of the data upon confirmation from the VCCS that the original data has been verified and archived or transferred successfully to an alternate processing system

E. **MALICIOUS CODE:** Contractor has used its best efforts through quality assurance procedures to ensure that there are no computer viruses or undocumented features in the Application accessed by the agency or its application users; and the Application does not contain any embedded device or code (e.g., time bomb) that is intended to obstruct or prevent any use of or access to the Application. Notwithstanding any rights granted under any resulting contract, agreement, purchase order, or scope of work or at law, Contractor hereby waives under any and all circumstances any right it may have or may hereafter have to exercise Electronic Self-Help or Acceptance Use Policy. Contractor agrees that the agency may pursue all remedies provided under law in the event of a breach or threatened breach of this Section, including injunctive or other equitable relief.

F. **PRIVACY AND SECURITY:** Contractor warrants that Contractor and its employees, Subcontractors, partners, and third-party providers have taken all necessary and reasonable measures to ensure that the Application, Licensed Services, contractor product, and any related deliverables do not include any degradation, known security vulnerabilities, or breach of privacy or security. Contractor agrees to notify the agency of any occurrence of such as soon as possible after discovery and provide the agency with fixes or upgrades for security vulnerabilities within 90 days of discovery.

G. **OPERATING SYSTEM AND SOFTWARE SUPPORTABILITY:** Contractor warrants that Contractor and its employees, Subcontractors, partners, and third-party providers have taken all necessary and reasonable measures to ensure that the Application, Licensed Services, contractor product, and any deliverables do not have dependencies on other operating systems or software that are no longer supported by Contractor, or its Subcontractors, partners, and third-party providers.

H. **ACCESS TO PRODUCT AND PASSWORDS:** Contractor warrants that the Application and Licensed Services do not contain disabling code or any program device or other undisclosed feature, including but not limited to, viruses, worms, trojan horses, or other code, which is designed to permit unauthorized access, delete, disable, deactivate, interfere with, or otherwise harm the Application, Licensed Services or the hardware or software of the agency or its application users. In addition, Contractor warrants that the agency and its application users will be provided commercially reasonable uninterrupted access to the Application. Contractor also warrants that it will not cancel or otherwise terminate access to the Application by disabling passwords, keys or tokens that enable continuous use of the Application by the agency and its application users during

the term of any Contract or any purchase order or scope of work issued hereunder. Contractor further warrants that the Application and Licensed Services are compatible with and will operate successfully on the equipment.

I. **OPEN SOURCE:** Contractor will notify the agency if the Application contains any Open-Source code.

J. **CONTRACTOR'S VIABILITY:** Contractor warrants that it has the financial capacity to perform and continue to perform its obligations under this Contract; that Contractor has no constructive or actual knowledge of any potential legal proceeding being brought against Contractor that could materially adversely affect performance of any resulting contract, purchase order or scope of work, and that entering into a Contract is not prohibited by any Contract, or order by any court of competent jurisdiction.

K. **CONTRACTOR'S PAST EXPERIENCE**: Contractor warrants that Contractor has provided the Licensed Services to a non-related third-party customer of Contractor without significant problems due to the Licensed Services, the Application, or Contractor.

L. **VULNERABILITY TESTING:** The security perimeter must be penetration tested on an annual basis by an independent third party for both infrastructure and application vulnerabilities. The hosted application must be tested for vulnerabilities during all stages of the quality assurance and testing processes before, during, and after deployment. Operating system and application platform software (middleware) must be tested for vulnerabilities on an ongoing basis to detect newly identified technical vulnerabilities

M. **CERTIFICATION:** Contractor must provide a copy of an independent security audit of the hosting facility attesting to the compliance of the facility with all applicable information security standards referenced in the agreement.

N. SOFTWARE EVOLUTION: Should contractor or software publisher merge or splinter the software previously provided to the VCCS, such action on the part of contractor or software publisher shall not in any way result in the VCCS being charged additional license or support fees in order to receive enhancements, releases, upgrade or support for the software. If contractor or software publisher reduces or replaces functionality contained in a licensed software product and provides the same or substantially similar functionality as or within a separate or renamed software product, then the VCCS shall be entitled to license such software product at no additional license or maintenance fee, and subject to the terms and conditions herein. If contractor or software publisher releases an option, future software product or other release that has substantially the same functionality as the software products provided under the contract, and software publisher and/or contractor ceases to provide maintenance for the older software product, then contractor shall offer the VCCS the option to exchange licenses for such replacement software product or function at no additional charge. Other than as set forth immediately above, there shall be no automatic or incidental license in favor of VCCS for new software and application products created by the Contractor during the Term.

O. NEW TECHNOLOGY:

I. Access to New Technology: Supplier will bring to Agency's attention any new products or services within the scope of the contract the Supplier believes will be of interest to Agency and will work to develop proposals for provisions of any such products or services as Agency requests.

II. New Services Offering Not Available from Supplier: If new or replacement products or services offerings become available and cannot be competitively provided by the supplier under the scope of this contract, Agency will have the right to purchase the new or replacement products or services from a third party. If Agency elects to use such new or replacement products or services offerings, Supplier will reasonably assist Agency to migrate to such products or services.

P. APPLICATION AND LICENSED SERVICE SUPPORT: At any time during the term of any order or SOW issued pursuant to this Contract, Supplier shall provide the following Application Services (including unlimited telephonic support and all necessary travel and labor) without additional charges to Agency in order to ensure such Agency and its Application Users are able to access and use the Application in accordance with the Requirements.

I. Coverage: Supplier shall provide Agency all reasonably necessary telephone or written consultation requested by such Agency in connection with use, problems, and operations of the application on a basis of 24 hours a day, seven (7) days a week.

II. Service Levels: Within one (1) hour of a request from VCCS, in its governance role, Supplier shall respond to such request for support of Licensed Services regarding the Application and Licensed Services., including Application, Supplier Product, and Documentation in accordance with the procedures identified in Exhibit 1 of the Contract, "Table of Service Levels, Response and Resolution Times and Escalation Procedures for Licensed Services". Agency may describe the problem by telephone, electronic mail, or vie a web site provided by Supplier.

III. Application Evolution: Should Supplier merge or splinter the Application previously provided to VCCS, such actions on the part of Supplier shall not in any way result in VCCS being charged additional license or support fees in order to access the Application, to enable its Application Users to access the Application, or to receive enhancements, releases, upgrades, or support for the application.

Q. TRAINING AND DOCUMENTATION:

I. Training: Supplier may make available, Supplier's fee, unless expressly excluded, includes all costs for any and all training as agreed upon for the training of at least VCCS trainers per order or SOW. In order to allow Agency the full benefit of the applicable Deliverable, the training will cover the use and operation of the Deliverable provided to Agency including instruction in any necessary conversion, manipulation, or movement of such VCCS's data. Supplier shall provide personnel sufficiently experienced and qualified to conduct such training at a time and location mutually agreeable to Supplier and Agency.

II. Documentation: Supplier shall deliver to Agency complete copies of any Documentation applicable to the Deliverable(s) provided to Agency, in a quantity and media format as agreed upon by the Parties under an order or SOW. Should Supplier revise or replace the Documentation, or should Documentation be modified to reflect Updates, Supplier shall deliver to Agency copies of the updated or replacement Documentation, in the same quantity and media format as originally requested by Agency, or as agreed upon between the Parties. Agency will have the right, as part of any license grant, to make as many additional copies of the Documentation, in whole or in part, for its own use as required. This Documentation must include, but is not limited to, overview descriptions of all major functions, detailed step-by-step installation and operating procedures for each screen and activity, and technical reference manuals. Such Documentation must be revised to reflect any modifications, fixes or updates made by Supplier. Agency, at its own discretion, will have the right, as part of the license granted by Supplier, to modify or completely customize all or part of the Documentation in support of the authorized use of the licensed Application or Software. The Agency may also duplicate such Documentation and include it in such Agency's document or platform. All Agency shall continue to include Supplier's copyright notice.

R. OFFEROR/CONTRACTOR PERFORMANCE MEASURES: The Virginia Community College System (VCCS) has developed a set of performance measures relating to Offeror's/Contractor's performance under this Contract and which are attached hereto and incorporated by reference as Exhibit 1. Offeror/Contractor agrees to be bound by and perform its obligations under this Contract pursuant to these performance measures. The remedies for the Contractor's failure to meet the performance measures are set forth in Exhibit 1.

Offeror/Contractor and Agency agree to meet within 30 calendar days of the Effective Date of this Contract to set forth the methodology and designated personnel of each Party to provide, collect, monitor, and report the performance measures data and mutually agreed-to incentives and remedies. Offeror/Contractor agrees to provide to Agency a report of its performance against the performance measures no less than once every six (6) months throughout the Contract Term. Offeror's/Contractor's report must include a comparison of its performance measures against the agreed-to targets and, in the event of any shortfall by Offeror/Contractor, proposed remediation measures. Offeror/Contractor will report its performance for the Contract in aggregate and for each order or SOW. Any instances of Offeror's/Contractor's non-compliance will be recorded in Offeror's/Contractor's Contract file and shared with Contract stakeholders. Offeror/Contractor further agrees that any degradation or failure of Offeror's/Contractor's performance obligations may result in failure to renew the Contract, termination for convenience of the Contract or termination for breach of the Contract. Agency will have all rights and remedies available by law.

Offerors seeking to add, delete, or modify any Terms or Conditions shall include such addition, deletion, or modification at the time of RFP Proposal submission. If an Offeror includes any other terms and conditions in its proposal, the VCCS reserves the right to accept or reject any such terms and conditions, to modify them through the negotiation process, and/or to consider those in the evaluation scoring of the proposals. At *NO TIME* after submission of the initial RFP response will the

VCCS agree to additional modifications, additions, or deletions of any general, Special, or IT terms and conditions.

Please note, exceptions or recommended language revisions to the liability provisions of the contract will not be considered at this time. If your firm is selected to go forward into negotiations, you will be required to state any exceptions to any liability provisions contained in the Request for Proposal and the VCCS Contract Template at that time via email to the designated VCCS Contracts Officer

No contract award can be made to any Supplier, for any Supplier products or services provided by Supplier, that are included on the U.S. Department of Homeland Security prohibition list in accordance with §2.2-2009 of the Code

XI. METHOD OF PAYMENT

Vendors shall submit proper invoices to invoice@ssc.vccs.edu or Virginia Community College System, Shared Services Center, ATTN: Accounts Payable; 147 Daleville Centre Drive, Daleville, VA 24083.

Payments for any resulting contract will be made by the VCCS in Accordance with Article 4 of the Virginia Public Procurement Act, Article 4 "Prompt Payment" (Code of Virginia §2.2-4347 et. seq.)

Payment will be made within 30 days of proper invoice. Payment may be made by check or electronic funds transfer.

XII. PRICING SCHEDULE

Complete "Attachment 6 – Pricing Schedule" for all services as outlined in this RFP.

XIII. ORDERING PROCEDURES

The VCCS will issue any/all purchase orders or SOWs through eVA.

XIV. ATTACHMENTS

The following attachments/exhibits must be completed and submitted as part of the proposal.

1. Attachment 1 - Vendor Data Sheet
2. Attachment 2 – State Corporation Commission Form
3. Attachment 3 – Proprietary and Confidential Information Form
4. Attachment 4 – Small Business Subcontracting Plan
5. Attachment 5 – Disclosure of AI Use in Proposal Development
6. Attachment 6 – Pricing Schedule
7. Attachment 7 – Information Security Requirements
8. Exhibit 1 – Offeror/Contractor Performance Measures
9. Exhibit 2 – Table of Service Levels, Response and Resolution Times and Escalation Procedures for Licensed Services

ATTACHMENT 1 – VENDOR DATA SHEET

This form must be returned with response to solicitation

Note: The following information is required as part of your response to this solicitation.
Qualification: The vendor must have the capability and capacity in all respects to satisfy fully all of the contractual requirements.
Vendor's Primary Contact:

Name:		Phone:		Email:	

Years in Business: Indicate the length of time you have been in business providing this type of good or service:

Years:		Months:	

Vendor Identification:

eVA Vendor ID:		DUNS Number:	

References: Indicate below five (5) references for whom you have performed similar services.

Reference #1			
Company:		Contact Name:	
Phone:		Email:	
Project:		Project $ Value:	
Dates of Service:		Notes:	

Reference #2			
Company:		Contact Name:	
Phone:		Email:	
Project:		Project $ Value:	
Dates of Service:		Notes:	

Reference #3			
Company:		Contact Name:	
Phone:		Email:	
Project:		Project $ Value:	
Dates of Service:		Notes:	

Reference #4			
Company:		Contact Name:	
Phone:		Email:	
Project:		Project $ Value:	
Dates of Service:		Notes:	

Reference #5			
Company:		Contact Name:	
Phone:		Email:	
Project:		Project $ Value:	
Dates of Service:		Notes:	

I certify the accuracy of this information.

Signed: _____ Date: _____

Name: _____ Title: _____

ATTACHMENT 2 – STATE CORPORATION COMMISSION FORM

This form must be returned with response to solicitation

Virginia State Corporation Commission ("SCC") registration information: **The undersigned Offeror:**

☐ is a corporation or other business entity with the following SCC identification number: _____
-OR-
☐ is not a corporation, limited liability company, limited partnership, registered limited liability partnership, or business trust
-OR-
☐ is an out-of-state business entity that does not regularly and continuously maintain as part of its ordinary and customary business any employees, agents, offices, facilities, or inventories in Virginia (not counting any employees or agents in Virginia who merely solicit orders that require acceptance outside Virginia before they become contracts, and not counting any incidental presence of the offeror in Virginia that is needed in order to assemble, maintain, and repair goods in accordance with the contracts by which such goods were sold and shipped into Virginia from offeror's out-of-state location)
-OR-
☐ is an out-of-state business entity that is including with this proposal an opinion of legal counsel which accurately and completely discloses the undersigned offeror's current contacts with Virginia and describes why those contacts do not constitute the transaction of business in Virginia within the meaning of § 13.1-757 or other similar provisions in Titles 13.1 or 50 of the Code of Virginia.

****NOTE** >>** Check the following box if you have not completed any of the foregoing options but currently have pending before the SCC an application for authority to transact business in the Commonwealth of Virginia and wish to be considered for a waiver to allow you to submit the SCC identification number after the due date for proposals (the Commonwealth reserves the right to determine in its sole discretion whether to allow such waiver): ☐

Signature: _____ Date: _____

Printed Name: _____

Title: _____

Name of Firm: _____

3/23/11

ATTACHMENT 3 – PROPRIETARY AND CONFIDENTIAL INFORMATION FORM

This form must be returned with response to solicitation

Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the *Virginia Freedom of Information Act*; however, the Offeror must invoke the protections of § 2.2-4342F of the *Code of Virginia*, in writing, either before or at the time the data or other material is submitted. The written notice must specifically identify the data or materials to be protected including the section of the proposal in which it is contained and the page numbers, and state the reasons why protection is necessary. The proprietary or trade secret material submitted in the original and all copies of the proposal 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. In addition, a summary of proprietary information submitted shall be submitted on this form. The classification of an entire proposal document, line item prices, and/or total proposal prices as proprietary or trade secrets is not acceptable. If, after being given reasonable time, the Offeror refuses to withdraw such a classification designation, the proposal will be rejected.

Name of Offeror (Firm):_____invokes the protections of § 2.2-4342F of the *Code of Virginia* for the following portions of my proposal submitted on_____.
Date

Signature: _____

Title: _____

☐ No portion of this proposal is to be considered confidential and/or proprietary.

DATA/MATERIAL TO BE PROTECTED	SECTION NO., & PAGE NO.	REASON WHY PROTECTION IS NECESSARY

ATTACHMENT 4 – SMALL BUSINESS SUBCONTRACTING PLAN

This form must be completed and returned with the bid.

Small Business Subcontracting Plan

It is the goal of the Commonwealth that over 42% of its purchases be made from small businesses. All potential offerors are required to return this document with their response.

Small Business: "Small business (including micro)" means a business which holds a certification as such by the Virginia Department of Small Business and Supplier Diversity (DSBSD) on the due date for proposals. This shall also include DSBSD-certified women-owned and minority-owned businesses and businesses with DSBSD service-disabled veteran owned status when they also hold a DSBSD certification as a small business on the proposal due date. Currently, DSBSD offers small business certification and micro business designation to firms that qualify.

Certification applications are available through DSBSD online at www.SBSD.virginia.gov (Customer Service).

Offeror Name: _____

Preparer Name: _____ **Date:** _____

Who will be doing the work: ☐ **I plan to use subcontractors** ☐ **I plan to complete all work**

Instructions

A. If you are certified by the DSBSD as a micro/small business, complete only Section A of this form.
B. If you are not a DSBSD-certified small business, complete Section B of this form. For the offeror to receive credit for the small business subcontracting plan evaluation criteria, the offeror shall identify the portions of the contract that will be subcontracted to DSBSD-certified small business for the initial contract period the initial contract period in Section B.

Offerors which are small businesses themselves will receive the maximum available points for the small business participation plan evaluation criterion, and do not have any further subcontracting requirements.
Offerors which are not certified small businesses will be assigned points based on proposed expenditures with DSBSD- certified small businesses for the initial contract period in relation to the offeror's total price for the initial contract period.

Points will be assigned based on each offeror's proposed subcontracting expenditures with DSBSD-certified small businesses for the initial contract period as indicated in Section B in relation to the offeror's total price.

Section A

If your firm is certified by the DSBSD provide your certification number and the date of certification.

Certification number:_____ Certification Date:_____

Section B

If the "I plan to use subcontractors' box is checked," populate the requested information below, per subcontractor to show your firm's plans for utilization of DSBSD-certified small businesses in the performance of this contract for the initial contract period in relation to the offeror's total price for the initial contract period. Certified small businesses include but are not limited to DSBSD-certified women-owned and minority-owned businesses and businesses with DSBSD service-disabled veteran-owned status that have also received the DSBSD small business certification. Include plans to utilize small businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc. It is important to note that this proposed participation will be incorporated into the subsequent contract and will be a requirement of the contract. Failure to obtain the proposed participation dollar value or percentages may result in breach of the contract.

C. **Plans for Utilization of DSBSD-Certified Small Businesses for this Procurement**

Subcontract #1

Company Name: _____ SBSD Cert #: _____

Contact Name: _____ SBSD Certification: _____ Contact

Phone: _____ Contact Email: _____

Value % or $ (Initial Term): _____ Contact Address: _____

Description of Work: _____

Subcontract #2

Company Name: _____ SBSD Cert #: _____

Contact Name: _____ SBSD Certification: _____ Contact

Phone: _____ Contact Email: _____

Value % or $ (Initial Term): _____ Contact Address: _____

Description of Work: _____

Subcontract #3

Company Name: _____ SBSD Cert #: _____

Contact Name: _____ SBSD Certification: _____ Contact

Phone: _____ Contact Email: _____

Value % or $ (Initial Term): _____ Contact Address: _____

Description of Work: _____

Subcontract #4

Company Name: _____ SBSD Cert #: _____

Contact Name: _____ SBSD Certification: _____ Contact

Phone: _____ Contact Email: _____

Value % or $ (Initial Term): _____ Contact Address: _____

Description of Work: _____

Subcontract #5

Company Name: _____ SBSD Cert #: _____

Contact Name: _____ SBSD Certification: _____ Contact

Phone: _____ Contact Email: _____

Value % or $ (Initial Term): _____ Contact Address: _____

Description of Work: _____

ATTACHMENT 5 – DISCLOSURE OF AI USE IN PROPOSAL DEVELOPMENT

This form must be returned with response to solicitation

Disclosure of AI Use in Proposal Development

Offerors are required to disclose the use of Artificial Intelligence (AI) tools, systems, or technologies during the development of their proposal. This disclosure must include:

- The specific AI tools or technologies utilized (e.g., generative AI, automated content creation tools, data analysis platforms).
- The purpose for which these tools were used in the proposal development process.

Offerors must ensure that all content, data, or analysis generated by AI tools has been reviewed and verified for accuracy and compliance with the requirements of this solicitation. *Failure to disclose the use of AI tools in the proposal development may result in disqualification or rejection of the proposal.*

Response:

By signing below, the Offeror acknowledges that they understand and accept the requirements regarding the disclosure and use of AI tools, systems, or technologies in the development of this proposal, as outlined above.

Signature: _____ Date: _____

Printed Name: _____

Title: _____

Name of Firm: _____

ATTACHMENT 6 – PRICING SCHEDULE

This form must be returned with response to solicitation

The successful offeror agrees to provide **SCOPE** in compliance with the Statement of Needs, General Terms and Conditions, Special Terms and Conditions, and IT Terms and Conditions for the prices stated below:

Vendor Name:	
Address:	

PRICING SHEET SCHEDULE:

Description	Cost (Provide Unit of Measure for each.)
Annual licensing	$
Installation and/or Integration	$
Maintenance & Support, if not included in licensing	$

** Add a pricing sheet that breaks down cost per year, including cost during renewal years.
** Provide specific information and additonal pricing as needed
** The pricing information supplied with your proposal must be valid for at least 120 calendar days from the submission date.
** Suppliers are encouraged to disclose pricing assumptions wherever possible. For example, if unit price is based on a certain volume, that assumption should be indicated. Suppliers are also encouraged to clearly identify any discount targets/ranges available. Aggregate discounts for all of the Commonwealth are requested.
** Your pricing proposal must include all charges of any kind associated with the Service. VCCS will not be liable for any fees or charges for the Service/Solution that are not set forth in the Excel Pricing Submittal. Any attempt to add these fees to submitted pricing will not be considered.

Virginia's Community Colleges Information Technology

Information Security Standard

19.1 – Public Cloud Services

Information Security Requirements

Version: 1.0

Status: Final 2017-01-25

Reference: ISO/IEC 27018:2014(E)

Contact: Chief Information Security Officer

PURPOSE

To establish a framework for information security management and practice by a provider of Public Cloud Services involving the security of VCCS data containing PII that may be accessed, processed, communicated to, or managed by the provider or any third-party service providers.

SCOPE

In accordance with ISO/IEC 27018:2014(E) a provider of Public Cloud Services is responsible to implement information security practices that provide protection of a customer's data assets by implementing information security practices that meet applicable legislation and regulations as well as contractual obligations. This Standard indicates the minimum expectations of a service provider when contracted by the VCCS to provide Public Cloud Services.

Public Cloud Services include any contract between the VCCS and a third-party for software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS).

APPLICABILITY

This Standard is applicable to all service providers who enter into a service contract with the VCCS to provide Public Cloud Services where VCCS owned data containing PII may be accessed, processed, communicated to, or managed by the service provider and by extension any business partners they may contract with whose services likewise access, process, communicate with, or managed VCCS owned data containing PII.

STANDARD

The requirements defined by this standard determine the minimum requirements for information security and data protection by a service provider of Public Cloud Services and associated business partners they may contract with who access, process, communicate, or manage VCCS owned data containing PII.

The Standard requires service provider to demonstrate they maintain an Information Security Program and engage in standard practices for Information Security that are equal to or more stringent than those followed by the VCCS. The Standard establishes the minimum acceptable requirements for protection of VCCS data by service providers and their business partners regardless of their currently adopted information security practices.

Requirement: § 19.1.1 – Legal, Statutory, Regulatory, and Contractual Requirements

This Standard indicates the minimum requirements for information security to be provided by a cloud services provider when contracted to provide public cloud services to any Virginia Community College System organization.

The cloud service provider must indicate in the contract for cloud services all information security responsibilities that will remain with the VCCS or are specifically excluded from their service offering depending on the type of service to be provided.

1. Any information security responsibilities not assigned to the VCCS or specifically excluded by contract will remain with the cloud service provider.
2. The cloud service provider and any third-party providers it may engage or contract with that access, process, communicate, or manage VCCS owned data will be required to sign a Non-Disclosure Agreement prior to service delivery.

The cloud service provider must comply with all Federal and Commonwealth of Virginia laws and regulations including the protection of client identifiable information, including:

- The Privacy Act of 1974
- Computer Matching and Privacy Protection Act of 1988
- E-Government Act of 2002
- US Internal Revenue Service (IRS) 1075 "Tax Information Security Guidelines For Federal, State and Local Agencies"
- National Institute of Standards and Technology (NIST) Guide for Protecting PII
- Code of VA Title 59.1 Trade and Commerce – Chapter 35 –Personal Information Privacy Act
- Virginia Department of Human Resources Management Policy 6.05 – Personnel Records Disclosure
- The Code of Virginia §2-2.2009

The VCCS requires a service level agreement (SLA) that will document its performance expectations of the cloud services provider, as well as its obligations under the cloud services contract.

Requirement: § 19.1.2 – Information Security Management System Requirements

The cloud service provider must provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

1. A set of policies for information security must be defined, approved by management, published and communicated to employees and relevant external parties.
    a. All hosted systems must be operated under the controls, security, and audit process of a SSAE16 / ISAE 3402 Type II SOC 2 hosting facility.
    b. The cloud service provider must provide the VCCS on an annual basis a copy of their current SOC 2 - Type II Audit Report obtained from an independent auditor as evidence that all relevant information security requirements for cloud services have been met.
        i. The (College/SO) ISO is responsible for reviewing the SOC 2 - Type II Audit Report against the requirements of this standard to ensure that the provider meets VCCS standards and has fulfilled its obligations under any agreement or contract with the VCCS.
2. The policies for information security must be reviewed at planned intervals not to exceed one year in duration or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Requirement: § 19.1.3 – Roles and Responsibilities

The cloud service provider must have an established management framework to initiate and control the implementation and operation of information security within the organization.

1. All information security responsibilities must be defined and allocated.
    a. The cloud services provider must designate the person responsible for Information Security at its hosting facility.
    b. The cloud services provider must designate a customer point of contact to facilitate customer success for the duration of the cloud services contract.
    c. The cloud services provider must notify the VCCS of any changes to its personnel responsible for the duties under the cloud services contract.
2. Conflicting duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
3. Appropriate contacts with relevant authorities must be maintained.
4. Appropriate contacts with special interest groups or other specialist security forums and professional associations must be maintained.
5. Information security must be addressed in project management, regardless of the type of project.

The cloud service provider must ensure the security of teleworking and use of mobile devices.

1. A policy and supporting security measures must be adopted to manage the risks introduced by use of mobile devices to access the provided cloud services.
2. A policy and supporting security measures must be implemented to protect information accessed, processed or stored at teleworking sites used by the cloud service provider's personnel.

Requirement: § 19.1.4 – Personnel Security

The cloud service provider must ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

1. Background verification checks on all candidates for employment who will have either physical or logical access to the VCCS data must be carried out by the cloud services provider in accordance with relevant laws, regulations and ethics and must be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
2. Contractual agreements between the cloud service provider and its employees and contractors must state their and the cloud service provider's responsibilities for information security.

The cloud service provider must ensure that employees and contractors are aware of and fulfill their information security responsibilities.

1. Management must require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
2. All employees of the organization and where relevant, contractors, must receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
3. There must be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

The cloud service provider must protect the VCCS's interests as part of the process of changing or terminating employment.

1. Information security responsibilities and duties that remain valid after termination or change of employment must be defined, communicated to the employee or contractor and enforced.

Requirement: § 19.1.5 – Asset Management

The cloud service provider must identify organizational assets and define appropriate protection responsibilities.

1. Assets associated with information and information processing facilities must be identified and an inventory of these assets must be drawn up and maintained.
2. Assets maintained in the inventory must be under the control or management of the service provider.
3. Rules for the acceptable use of information and of assets associated with information and information processing facilities must be identified, documented and implemented.
4. All employees and external party users must return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

The cloud service provider must ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

1. Information must be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.
2. An appropriate set of procedures for information labelling must be developed and implemented in accordance with the information classification scheme adopted by the organization.

3. Procedures for handling assets must be developed and implemented in accordance with the information classification scheme adopted by the organization.

The cloud service provider must prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

1. Procedures must be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
2. Media must be disposed of securely when no longer required, using formal procedures.
3. Media containing information must be protected against unauthorized access, misuse or corruption during transportation.

Requirement: § 19.1.6 – Access Control

The cloud service provider must limit access to information and information processing facilities.

1. An access control policy must be established, documented and reviewed based on business and information security requirements.
    a. Where appropriate, the public cloud service provider must enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.
2. Users must only be provided with access to the network and network services that they have been specifically authorized to use.

The cloud service provider must ensure authorized user access and prevent unauthorized access to systems and services.

1. A formal user registration and de-registration process must be implemented to enable assignment of access rights.
2. A formal user access provisioning process must be implemented to assign or revoke access rights for all user types to all systems and services.
3. The allocation and use of privileged access rights must be restricted and controlled.
4. The allocation of secret authentication information must be controlled through a formal management process.
5. Asset owners must review users' access rights at regular intervals.
6. The access rights of all employees and external party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, or adjusted upon change.

The cloud service provider must require users to be accountable for safeguarding their authentication information.

1. Users must be required to follow the VCCS practices in the use of secret authentication information (password, passphrase, pin number, two-factor security code).

The cloud service provider must prevent unauthorized access to systems and applications.

1. Access to information and application system functions must be restricted in accordance with the access control policy.
    a. The cloud services provider must provide a secure perimeter and operating environment that includes a security plan for firewall intrusion detection, vulnerability assessments, penetration analysis, and incident management.
    b. Access to system software and databases must be controlled by unique identifiers assigned to each person with system access to ensure accountability, audit trails and periodic password changes.
    c. Penetration testing must occur on an annual basis and the results reported to the VCCS Chief Information Security Officer or the College Information Security Officer.
2. Where required by the access control policy, access to systems and applications must be controlled by a secure log-on procedure.
3. Password management systems must be interactive and must ensure quality passwords.
    a. If the hosted solution does not use Federated Identify and Access Management for Single-Sign On authentication, then passwords must meet the following complexity and expiration requirements as a minimum:
        - Passwords must have a minimum of 8 characters and must require at least 1 capital letter, 1 numeric character, 1 punctuation or special character
        - Passwords cannot match the logon name or identification
        - Passwords cannot use more than two sequential or repeating characters.
        - Passwords must expire after 180 days maximum
        - Password reuse must disallow the last 12 passwords
        - The maximum number of failed logon attempts is 5 after which the account is locked
        - Account lockouts must be reset by an administrator
4. The use of utility programs that might be capable of overriding system and application controls must be restricted and tightly controlled.
5. Access to program source code must be restricted.

Requirement: § 19.1.7 – Data Protection

The cloud service provider must ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

1. A policy on the use of cryptographic controls for protection of information must be developed and implemented.
    a. All VCCS data in transit must be encrypted with a minimum 128 bit SSL Certificate.
    b. Work papers (attachments) within a database must be encrypted using AES-256 (Advanced Encryption Standard) encryption as a minimum.
    c. Access via the Internet must use Hypertext Transport Protocol Secure (https).
    d. The public cloud PII processor must provide information to the VCCS regarding the circumstances in which it uses cryptography to protect the PII it processes.
2. A policy on the use, protection and lifetime of cryptographic keys must be developed and implemented through their whole lifecycle.

a. All cryptographic keys must be backed up with copies stored at an offsite location.

Requirement: § 19.1.8 – Physical and Environmental Security

The cloud service provider must prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

1. Security perimeters must be defined and used to protect areas that contain sensitive or critical information and information processing facilities.
    a. The cloud service provider must incorporate a "defense in depth" strategy for access to all information and information processing facilities.
    b. All information processing facilities that process, store, distribute, or manage VCCS data must be physically located within the borders of the continental United States.
2. Secure areas must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
3. Physical security for offices, rooms and facilities must be designed and applied.
    a. Provide adequate barriers, alarm systems, and supervised access control systems to ensure control of physical access to all such facilities.
4. Physical protection against natural disasters, malicious attack or accidents must be designed and applied.
    a. Information processing facilities must be protected against fire, flooding, and weather related damage or destruction.
5. Procedures for working in secure areas must be designed and applied.
6. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The cloud service provider must prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

1. Equipment must be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
2. Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.
3. Power and telecommunications cabling carrying data or supporting information services must be protected from interception, interference or damage.
4. Equipment must be correctly maintained to ensure its continued availability and integrity.
5. Equipment, information or software must not be taken off-site without prior authorization.
6. Security must be applied to off-site assets taking into account the different risks of working outside the organization's premises.
7. All items of equipment containing storage media must be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
8. Users must ensure that unattended equipment has appropriate protection.

9. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities must be adopted.

Requirement: § 19.1.9 – Operations Security

The cloud service provider must ensure correct and secure operations of information processing facilities.

1. Operating procedures must be documented and made available to all users who need them.
2. Changes to the organization, business processes, information processing facilities and systems that affect information security must be controlled.
3. The use of resources must be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.
4. Development, testing, and operational environments must be separated to reduce the risks of unauthorized access or changes to the operational environment.

The cloud service provider must ensure that information and information processing facilities are protected against malware.

1. Detection, prevention and recovery controls to protect against malware must be implemented and combined with appropriate user awareness.

The cloud service provider must protect against loss of data.

1. Backup copies of information, software and system images must be taken and tested regularly in accordance with an agreed backup policy.
    a. All production databases must be backed up nightly and then copied electronically to a remote SSAE 16 type II facility.
    b. Full system backups must be retained for two weeks minimum. The VCCS requires a minimum of a weekly full system backup and incremental daily backups for all application environments (Production, Test, and Development).

The cloud service provider must record events and generate evidence.

1. Event logs recording user activities, exceptions, faults and information security events must be produced, kept and regularly reviewed and monitored.
    a. All servers must be monitored 24/7/365 with system alerts sent to the application hosting support engineers (excessive CPU, low disc space, application pool failures, etc.).
    b. Maintain logs of all end-user attempts to gain system access.
    c. Maintain logs of all failed end-user attempts to gain system access.
    d. Generate high-priority alerts to designated users in the event of a security event.
    e. Provide the ability to query all system logs.
    f. Provide the ability to monitor the system for security breaches and intrusions.
    g. Log all breaches of system security.
2. Logging facilities and log information must be protected against tampering and unauthorized access.
3. System administrator and system operator activities must be logged and the logs protected and regularly reviewed.

4. The clocks of all relevant information processing systems within an organization or security domain must be synchronized to a single reference time source.

The cloud service provider must ensure the integrity of operational systems.

1. Procedures must be implemented to control the installation of software on operational systems.

The cloud service provider must prevent exploitation of technical vulnerabilities.

1. Information about technical vulnerabilities of information systems being used must be obtained in a timely fashion and the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.
2. Rules governing the installation of software by users must be established and implemented.

The cloud service provider must minimize the impact of audit activities on operational systems.

1. Audit requirements and activities involving verification of operational systems must be carefully planned and agreed to minimize disruptions to business processes.

Requirement: § 19.1.10 – Communications Security

The cloud service provider must ensure the protection of information in networks and its supporting information processing facilities.

1. Networks must be managed and controlled to protect information in systems and applications.
    a. The cloud service hosting facility must provide a N+1 network infrastructure that includes connectivity to at least 2 unique telecom providers for Internet access.
    b. Availability of Internet connectivity must be covered by a 99.9% Service Level Agreement.
2. Security mechanisms, service levels and management requirements of all network services must be identified and included in network services agreements, whether these services are provided in-house or outsourced.
3. Groups of information services, users and information systems must be segregated on networks.

The cloud service provider must maintain the security of information transferred within an organization and with any external entity.

1. Formal transfer policies, procedures and controls must be in place to protect the transfer of information through the use of all types of communication facilities.
2. Agreements must address the secure transfer of business information between the organization and external parties.
3. Information involved in electronic messaging must be appropriately protected.
4. Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information must be identified, regularly reviewed and documented.

Requirement: § 19.1.11 – System Acquisition, Development and Maintenance

The cloud service provider must ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

1. The information security related requirements must be included in the requirements for new information systems or enhancements to existing information systems.
2. Information involved in application services passing over public networks must be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
3. Information involved in application service transactions must be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

The cloud service provider must ensure that information security is designed and implemented within the development lifecycle of information systems.

1. Rules for the development of software and systems must be established and applied to developments within the organization.
    a. Software developed by the cloud service provider shall be designed to comply with, as applicable, the Commonwealth Enterprise Architecture Standard (EA 225) as defined at: http://www.vita.virginia.gov/library/
    b. Software developed by the cloud service provider shall be designed to comply with, as applicable, the Virginia Information Technology Accessibility Standard (GOV 103) as defined at: http://www.vita.virginia.gov/library/
    c. If applicable, the solution shall comply with all current COV Data Standards, as applicable to the project - as described on: http://www.vita.virginia.gov/library/
    d. All software solutions provided by the cloud services provider for use by the VCCS shall be designed to function using the most recently certified versions of the following web browsers, at a minimum: Internet Explorer, Firefox, Chrome, and Safari and shall be backwardly compatible with currently supported versions.
2. Changes to systems within the development lifecycle must be controlled by the use of formal change control procedures.
    a. The patches and upgrades to operating or application software shall be scheduled during normal maintenance windows (weeknights) during non-critical times.
3. When operating platforms are changed, business critical applications must be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
4. Modifications to software packages must be discouraged, limited to necessary changes and all changes must be strictly controlled.
5. Principles for engineering secure systems must be established, documented, maintained and applied to any information system implementation efforts.
6. Organizations must establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
    a. If VCCS related custom integrations are required by the cloud services, the cloud service provider's solution must include the hosting of three complete separate environments (landscapes): development, test, and production.

7. The cloud service provider must supervise and monitor the activity of outsourced system development to ensure that all applicable information security requirements are met.
8. Testing of security functionality must be carried out during development.
9. Acceptance of testing programs and related criteria must be established for new information systems, upgrades and new versions.

The cloud service provider must ensure the protection of data used for testing.

1. Test data must be selected carefully, protected and controlled.

Requirement: § 19.1.12 – Supplier Relationships

The cloud service provider must ensure protection of the organization's assets that is accessible by suppliers.

1. Information security requirements for mitigating the risks associated with supplier's access to the organization's assets must be agreed upon with the supplier and documented.
2. All relevant information security requirements must be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
3. Agreements with suppliers must include requirements to address the information security risks associated with information and communications technology services and product supply chain.

The cloud service provider must maintain an agreed level of information security and service delivery in line with supplier agreements.

1. Organizations must regularly monitor, review and audit supplier service delivery.
2. Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, must be managed, taking into account the criticality of business information, systems and processes involved and re-assessment of risks.

Requirement: § 19.1.13 – Information Security Incident Management

The cloud service provider must ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

1. Management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.
2. Information security events must be reported through appropriate management channels as quickly as possible.
    a. The VCCS CISO or College ISO must be notified as soon as any breach of its data through unauthorized access is detected.
3. Employees and contractors using the organization's information systems and services must be required to note and report any observed or suspected information security weaknesses in systems or services.
4. Information security events must be assessed and it must be decided if they are to be classified as information security incidents.

5. Information security incidents must be responded to in accordance with the documented procedures.
6. Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.
7. The organization must define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Requirement: § 19.1.14 – Business Continuity

Information security continuity must be embedded in the cloud service provider's business continuity management systems.

1. The cloud service provider must determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.
2. The cloud service provider must establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.
3. The cloud service provider must verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

The cloud service provider must ensure availability of information processing facilities.

1. Information processing facilities must be implemented with redundancy sufficient to meet availability requirements.
    a. All utilities (electrical power, telecommunications, and heating, ventilation, and air conditioning) and relevant components of the data center operation serving the cloud service providers hosting facility must have N+1 redundancy capable of maintaining the availability of the cloud services to meet service level agreements with the VCCS.
    b. The cloud service shall be designed to provide full system redundancy/fail-over to a remote site within the timeframe established by the business for disaster recovery in the event that service outages or other application problems impact users for 48 hours or longer.

Requirement: § 19.1.15 – Compliance

The cloud service provider must avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and security requirements.

1. All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements must be explicitly identified, documented and kept up to date for each information system and the organization.
2. Appropriate procedures must be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
3. Records must be protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.
4. Privacy and protection of personally identifiable information must be ensured as required in relevant legislation and regulation where applicable.

5. Cryptographic controls must be used in compliance with all relevant agreements, legislation, and regulations.

The cloud service provider must ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

1. The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) must be reviewed independently at planned intervals or when significant changes occur.
2. Managers must regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.
3. Information systems must be regularly reviewed for compliance with the organization's information security policies and standards.

Requirement: § 19.1.16 – Consent and choice

The public cloud services provider must provide the VCCS with the means to enable them to fulfill their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

Requirement: § 19.1.17 – Purpose legitimacy and specification

Data to be processed under a contract should not be processed for any purpose independent of the instructions of the VCCS.

1. VCCS data remains the property of the VCCS and may not be used for any purpose except that for which it is expressly authorized.
    a. VCCS data may not be used by the cloud services provider for sales, marketing, advertising, analysis, or any other purpose except as approved by the VCCS.

Requirement: § 19.1.18 – Secure erasure of temporary files

Temporary files and documents must be erased or destroyed within a specified, documented period.

1. Information systems may create temporary files in the normal course of their operation. Such files are specific to the system or application but may include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they may not be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used.
    a. Regardless of the need for temporary files, a copy of all VCCS data must be returned to the VCCS in machine readable format at the end of the contract and all remaining data must be immediately erased from the cloud service provider's systems, storage media, and backups.

Requirement: § 19.1.19 – Use, retention and disclosure limitation

The contract between the public cloud services provider and the VCCS must require the public cloud services provider to notify the VCCS, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.

1. The public cloud PII processor must provide contractual guarantees that it will reject any requests for PII disclosure that are not legally binding, consult the VCCS where legally permissible before making any PII disclosure and accept any contractually agreed requests for PII disclosures that are authorized by the VCCS.

Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.

1. The records should include the source of the disclosure and the source of the authority to make the disclosure.

Requirement: § 19.1.20 – Openness, transparency and notice

The use of sub-contractors by the public cloud services provider to process PII should be disclosed to the relevant cloud service customers before their use.

1. Provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud services provider and the VCCS.
    a. The contract must specify that sub-contractors may only be commissioned on the basis of a consent that can generally be given by the VCCS at the beginning of the service.
    b. The public cloud services provider must inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.

2. Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub-contractors, but not any business-specific details. The information disclosed must also include the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud service processor.
3. Where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer.

Requirement: § 19.1.21 – Accountability

The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure, or alteration of PII.

1. In the event of a data breach involving PII, the public cloud services provider will provide the information necessary for the cloud service customer to fulfill its obligation to notify relevant authorities.

Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).

1. In the absence of more restrictive requirements, the cloud services provider shall retain all records related to a security breach for a minimum of five years.

The public cloud PII processor must have a policy in respect to the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

1. In the event the contract for services is terminated by either party, the cloud services provider shall return all data to the VCCS in machine readable format and shall certify that no data remains in the possession of the cloud services provider or any sub-contractors.
2. The cloud services provider shall erase all VCCS data from any location where the data may be stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the VCCS using commercial forms of erasure to be agreed to by the VCCS.

Requirement: § 19.1.22 – Information security

Individuals under the public cloud service provider's control with access to PII should be subject to a confidentiality obligation.

1. A confidentiality agreement, in whatever form, between the public cloud services provider, its employees and its agents must ensure that employees and agents do not disclose PII for purposes independent of the instructions of the cloud service customer. The obligations of the confidentiality agreement must survive termination of any relevant contract.

The creation of hardcopy material displaying PII must be restricted.

1. All hardcopy of VCCS data that contains PII is forbidden without the express consent of the VCCS in writing and must be tracked and destroyed when the purpose for which the hardcopy was created has been fulfilled.

The cloud services provider must follow a documented procedure for, and retain a log of, data restoration efforts.

PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).

1. Copies of VCCS data on removable media must not be made except at the written request of the VCCS or to facilitate backup and business continuity operations.

Portable physical media and portable devices that do not permit encryption must not be used.

1. The VCCS requires that all data on portable media be encrypted.

PII that is transmitted over public data-transmission networks must be encrypted prior to transmission.

1. The VCCS requires that all data in transit or at rest must be encrypted when accessed over a public data-transmission network.

Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

1. The VCCS requires that all hardcopy to be destroyed must be processed by a certified data destruction vendor and that logs be kept to document what has been destroyed, when, and by whom.

If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication, and authorization purposes.

1. VCCS requires that all users have a distinct user ID and that elevated privilege users have separate user IDs for occasions when privileged access is required. Shared use of user accounts is prohibited.

An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.

1. Cloud service provider personnel having access to PII must be reviewed on a quarterly basis or more frequently when personnel changes occur to ensure that only persons with a legitimate need have access to PII data.

De-activated or expired user IDs must not be granted to other individuals.

Contracts between the cloud service customer and the public cloud PII processor must specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the VCCS. Such measures are not to be subject to unilateral reduction by the public cloud services provider.

Contracts between the public cloud service providers and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures must not be subject to unilateral reduction by the sub-contractor.

The public cloud services provider should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

Requirement: § 19.1.23 – Privacy compliance

The public cloud services provider must specify and document the locations in which PII might possibly be stored.

1. The VCCS requires that all VCCS data reside within the borders of the continental United States. This includes both primary data center facilities and backup or secondary data center facilities and all locations where data may be stored for backup purposes.

PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

1. This requirement is in addition to the requirement to encrypt data while in transit.

Related Documents

VCCS Information Security Policy

VCCS IT Security Standards

ISO/IEC 27000 Information security management systems

ISO/IEC 27001 Information security management systems — Requirements

ISO/IEC 27002 Code of practice for information security controls

ISO/IEC 27003 Information security management system implementation guidance

ISO/IEC 27004 Information security management — Measurement

ISO/IEC 27005 Information security risk management

ISO/IEC 27014 Governance of information security

ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

EXHIBIT 1

OFFEROR/CONTRACTOR PERFORMANCE MEASURES

TABLE OF PERFORMANCE LEVELS AND REMEDIES

Service Level (monthly)	Service Level Remedies (Prorated Fees Monthly)
Above 99.9%	0%
98.99 - 97%	10%
96.99 – 95%	15%
94.99 – 93%	30%
92.99 – 90%	50%
Below 90%	100% and at VCCS's sole discretion, Termination of the Contract

EXHIBIT 2

TABLE OF SERVICE LEVELS, RESPONSE AND RESOLUTION TIMES

AND ESCALATION PROCEDURES FOR LICENSED SERVICES

Severity (Sample Problems)	**Response Time**	**Resolution Time (Fix/work-around within)**	**Internal Escalation Procedure**
1 (Application down)			
2 (certain processing interrupted or malfunctioning but Application is able to process)			
3 (minor intermittent malfunctioning, Application able to process data)			