Maine Community College System

323 State Street
Augusta, ME 04330

Competitive Bid
Request for Proposal
This is NOT an order.

Sensitive Data Discovery / DLP Solution

Issue Date:	**May 26, 2021**
Questions from Bidders Due:	**June 10, 2021, 12pm EST**
Response Due Date:	**June 18, 2021, 1pm EST**
Return Proposal To:	**Scott Fortin** **Chief Information Security Officer** **Maine Community College System** **323 State Street** **Augusta, ME 04330** **207.629.4004** **sfortin@mccs.me.edu**

Table of Contents

1.0 Background & Introduction

This Request for Proposal (RFP) is issued by the Maine Community College System (MCCS) to solicit proposals from qualified, experienced, financially sound, and responsible firms to establish a contract through competitive negotiations for a new, innovative software tool to assist information technology and information security staff with protecting sensitive data as required by MCCS policy as well as state and federal law.

MCCS is made up of the seven accredited community colleges across the state of Maine. Over 16,000 students were enrolled in credit course in Fall 2019, with two-thirds of the students being enrolled in career and occupational programs. In addition to the degree programs, the colleges also provide an extensive array of Continuing Education and Workforce Development training to individuals across the state. The mission of MCCS is to provide associate degree, diploma and certificate programs directed at the educational, career and technical needs of the State's citizens and the workforce needs of the State's employers. The primary goals of the System are to create an educated, skilled and adaptable labor force that is responsive to the changing needs of the economy of the State and to promote local, regional and statewide economic development.

The purpose of this RFP is to provide interested parties with information to enable them to prepare and submit proposals for a comprehensive Sensitive Data Discovery / DLP Solution, including a hosted environment and all other requested services and support. MCCS intends to use the results of this RFP to award a contract for these products and services.

The term of the contract shall be for a period of three (3) years from the date of contract execution. There may be two (2) one-year renewals for a total of five (5) years at the option of MCCS.

At a minimum, MCCS requires the solution address the following high-level requirements, explored further in section 6.1:

1. Scan college systems to identify PII, CUI, PHI, and other sensitive forms of data.
2. Report findings to information technology / information security personnel through a variety of communication methods.
3. Remediate sensitive data incidents- either natively or through extensibility features (API, partner solutions, etc.)
4. Simplify management of the solution through automation, intuitive interfaces, and scalable installation methods.
5. Align the solution with a multi-college distributed computing environment.
6. Support the solution through a variety of communication methods and knowledge sources.

Preference will be given to proposals conforming to the specifications provided; however, alternate recommendations may be considered. If a vendor chooses to make inquiries on the specifications provided, the rules set forth in **Section 9.0, Interpretation of Contract Documents** apply. MCCS reserves the right to accept or reject any or all of the proposals received, in part or in whole.

Additionally, please refer to **Attachment B: Standard Terms and Conditions Applicable to All MCCS Contracts**.

2.0 Schedule & Deadlines

Event	**Date and time**
MCCS issues RFP	May 26, 2021
Questions from Bidders Due	June 10, 2021 – 12 PM EST
Answer returned to Bidders (Via RFP Addendum)	June 11, 2021 – 5 PM EST
RFP Due Date	June 18, 2021 - 1 PM EST
Selected Vendor Presentations	June 24 and/or June 25, 2021
Recommendation Submitted to CFO	June 29, 2021
Notification of Award	June 30, 2021
Contract Start Date	TBD, FY22 (July 1, 2021 – June 30, 2022)

Please note: **MCCS retains the right to change any dates and times.**

3.0 Examination of Specification and Schedule

Each bidder or his or her authorized agent is expected to examine the bid specifications, contract documents, and all other instructions pertaining to this RFP. Failure to do so will be at the bidder's own risk, and the bidder cannot secure relief on the plea of error in the bid. MCCS reserves the right to accept or reject any and all bids in part or in whole.

4.0 Submission Instructions

4.1 Proposal Transmission

Electronic submission through email is the required method of delivering your proposal.

- Email proposals should be sent to sfortin@mccs.me.edu

- The Email Subject line must read "MCCS Sensitive Data Discovery / DLP Solution Response"
- The emailed proposal must be RECEIVED no later than 1 PM EST on June 18, 2021.
- MCCS will acknowledge receipt of all proposals sent through email within one business day.
- It is the bidder's responsibility to ensure that its proposal is received in its entirety by the proposal due date and time. Any bid received after the date and time specified will not be accepted, read, or evaluated.
- MCCS will not be responsible for computer, server, Internet or any technical problems, errors, delivery delays, or failures beyond its physical control. Bidders are advised to send their bid responses before the bid deadline to avoid potential delays.
- The MCCS account receiving the submissions is limited to receive emails up to 50 MB in size. If your response is larger than 50 MB, please split your response into separate emails, and indicate in the subject line that you are doing so. All emails containing any part of your bid response must be received before the bid deadline.

4.2 Modification or Withdrawal of Offers

The bidder's authorized representative may withdraw or modify their proposal, prior to the due date. Modification to, or withdrawal of, a proposal received by MCCS after the exact hour and date specified for receipt of proposals will not be considered.

4.3 Pricing

Pricing on this RFP must be firm and remain open for a period of not less than 180 days from the proposal due date. Any attempt to manipulate the format of the document, attach caveats to pricing, or submit pricing that deviates from the current format will put your proposal at risk.

4.4 Vendor Presentations

Vendors may be requested to provide a presentation of their proposal, which would include a detailed analysis of how each of the bid requirements would be satisfied should the bidder receive the award. Vendor presentations are tentatively scheduled for June 24 and/or June 25, 2021. These presentations will not be open to the public.

4.5 Pre-Award Discussions

After the proposals are opened, but before the award, MCCS may elect to engage in discussions with any or all of the proposal respondents for purposes of:

- Resolving minor differences
- Clarifying necessary details and responsibilities
- Emphasizing important issues and points
- Receiving formal assurances from said respondents

MCCS may request best and final offers from those bidders determined by MCCS to be reasonably viable for contract award. However, MCCS reserves the right to award a contract on the basis of initial proposals received. Therefore, each proposal should contain the bidder's best terms from a price and technical standpoint.

Following evaluation of the best and final offers, MCCS may select for final contract negotiations/execution the offers that are most advantageous to MCCS, considering cost and the evaluation criteria in this RFP.

4.6 Proposal Requirements

To be considered complete, each proposal must include the following:

- ☐ Cover page with company name, proposal principal authors, date, company address and company URL
- ☐ Primary contact(s) with phone number and e-mail address(es)
- ☐ The bid should be dated and signed by an officer of your company with the authority to approve the submission of the proposal
- ☐ Section labeled BUSINESS PROPOSAL as described in Section 5
- ☐ Section labeled TECHNICAL PROPOSAL as described Section 6.1
- ☐ Section labeled SECURITY as described in Section 6.2
- ☐ Section labeled SPECIAL CONSIDERATION as described in Section 6.3
- ☐ Section labeled TRAINING PROPOSAL
- ☐ Section labeled COST PROPOSAL

5.0 BUSINESS PROPOSAL

The Business Proposal must address the following topics except those specifically identified as "optional."

5.1 General (optional)

This section of the business proposal may be used to introduce or summarize any information the Respondent deems relevant or important to the successful acquisition of the products and/or services requested in this RFP.

5.2 Respondent's Company Structure

The legal form of the Respondent's business organization, the state in which formed (accompanied by a certificate of authority), the types of business ventures in which the organization is involved, and a chart of the organization are to be included in this section. If the organization includes more than one product division, the division responsible for the development and marketing of the requested products and/or services in the United States must be described in more detail than other components of the organization.

5.3 Company Financial Information

This section must include the Respondent's financial statement, including an income statement and balance sheet, for each of the two most recently completed fiscal years. The financial statements must demonstrate the Respondent's financial stability. If the financial statements being provided by the Respondent are those of a parent or holding company, additional financial information should be provided for the entity/organization directly responding to this RFP.

5.4 Contract

Any or all portions of this RFP and any or all portions of the bidder's response may be incorporated as part of the final contract.

5.5 References

The Respondent must include a list of at least three (3) clients for whom the Respondent has provided products and/or services that are the same or similar to those products and/or services requested in this RFP. Information provided should include the name, address, and telephone number of the client facility and the name, title, and phone of a person who may be contacted for further information.

5.6 Subcontractors

The bidder is responsible for the performance of any obligations that may result from this RFP, and shall not be relieved by the non-performance of any subcontractor. Any bidder's proposal must identify all subcontractors and describe the contractual relationship between the bidder and each subcontractor. Either a copy of the executed subcontract or a letter of agreement over the official signature of the firms involved must accompany each proposal.

Any subcontracts entered into by the bidder must comply with MCCS statutes and will be subject to the provisions thereof. For each portion of the proposed products or services to be provided by a subcontractor, the technical proposal must include the identification of the functions to be provided by the subcontractor and the subcontractor's related qualifications and experience.

The combined qualifications and experience of the bidder and any or all subcontractors will be considered in the RFP evaluation. The Respondent must furnish information to MCCS as to the amount of the subcontract, the qualifications of the subcontractor for guaranteeing performance, and any other data that may be required by MCCS. All subcontracts held by the bidder must be made available upon request for inspection and examination by appropriate MCCS officials, and such relationships must meet with the approval of MCCS.

The bidder must list any subcontractor's name, address and the state in which formed that are proposed to be used in providing the required products or services. The subcontractor's responsibilities under the proposal, the anticipated dollar amount for subcontract, the subcontractor's form of organization, and an indication from the subcontractor of a willingness to carry out these responsibilities are to be included for each subcontractor. This assurance in no way relieves the bidder of any responsibilities in responding to this RFP or in completing the commitments documented in the proposal.

5.7 General Information

Each Respondent must enter your company's general information including contact information.

5.8 Experience Serving Higher Education Institutions / Similar Clients

Each Respondent is asked to please describe your company's experience in serving clients of a similar size to the Maine Community College System that also had a similar scope. Please provide specific clients and detailed examples. Please remember the seven colleges of the Maine Community College System are each individually accredited institutions.

5.9 Value Added Offerings

MCCS is always considering creative, cost-effective solutions to increase efficiencies and decrease expenditures. Does your company offer integrated service programs that will add value to the contract? Please describe the details of the program including cost, structure, and the benefits to be realized by MCCS as an alternative to the proposal for consideration.

6.0 TECHNICAL PROPOSAL

The Technical Proposal must be divided into the sections as described below. Every point made in each section must be addressed in the order given. The same outline numbers must be used in the response. RFP language should not be repeated within the response. Where appropriate, supporting documentation may be referenced by a page and paragraph number. However, when this is done, the body of the technical proposal must contain a meaningful summary of the referenced material. The referenced document must be included as an appendix to the technical proposal with referenced sections clearly marked. If there are multiple references or multiple documents, these must be listed and organized for ease of use by MCCS.

6.1 Functional Requirements

Scan college systems to identify PII, CUI, PHI, and other sensitive forms of data.

The MCCS utilizes a diverse range of systems to achieve operational goals. Below are requirements that will help us determine if your solution supports sensitive data scanning for our college IT systems:

- ❑ Provide the ability to scan unstructured data at rest that resides on Windows servers and file shares (including a Microsoft Distributed File Server (DFS) environment).
- ❑ Provide the ability to scan Windows and Mac OS endpoints.
- ❑ Provide the ability to scan Linux servers and endpoints.
- ❑ Provide built in scan conditions for common types of data: HIPAA, PCI-DSS, GDPR, and others, especially those related to higher education
- ❑ Allow for custom scans policies to be created with granular search terms
- ❑ Possess capability to scan images, using Optical Character Recognition (OCR), including TIFF, PDF, BLOB, JPEG, GIF, and PNG files.
- ❑ Possess capability to search common file types including but not limited to Microsoft Office (Word, Excel, PowerPoint, Access), Office Open Document Format (general), Adobe Creative Suite,
- ❑ Does your solution scan compressed files and volumes?
- ❑ Provide the ability to limit CPU, memory, network, and disk resources a scan consumes during certain times.
- ❑ Provide the ability to set scheduling for the automatic execution of scan times.
- ❑ Describe the process of resuming a scan in the event the scan in disrupted because the client went offline. Does the scan have to start at the beginning again?
- ❑ Does your solution provide the ability to perform full, differential, and/or incremental scans of data at rest?
- ❑ What features or methods does your solution employ to aid in minimizing false positives?
- ❑ Does your solution have a file size limit in which it scans?
- ❑ Does your solution have the ability to do form recognition?
- ❑ If your solution provides file fingerprinting, please describe how the solution utilizes this feature.
- ❑ Does your solution provide information on what users have access to a file or folder that has been found to contain sensitive protected data?

The abridged inventory below (with 5/8 institutions reporting) may help to provide context on the types of systems that will be scanned using a Sensitive Data Discovery / DLP tool:

Device Type	OS	Version	Quantity
Endpoint	*Windows*	*10*	*1750*
Endpoint	*Mac OS*	*10.15 & 11*	*50*
Server	*Windows*	*2019*	*221*
Server	*Linux*	*CentOS 8*	*10*

Report findings to information technology / information security personnel through a variety of communication methods.

Once sensitive data is found by the proposed solution, notification must be sent to the appropriate IT/IS personnel in order to remedy the situation (discussed further in Remediate). The following requirements will help us determine if alerts generated by the SDD/DLP solution will integrate with daily IT support operations:

- ❑ Provide detailed, exportable, custom reports that displays the location of where the sensitive protected data is within the data at rest, as well as what security policy that data violates.
- ❑ Employ security measures to limit visibility of reported data content found during the scans to only authorized users.
- ❑ Integrate with security information and event management (SIEM) systems (email/syslog submission at a minimum)
- ❑ Integrate with work order / ticketing systems (email submission at a minimum)
- ❑ Send email/SMS alerts that can be tuned by severity.
- ❑ Report files that could not be scanned because of encryptions or incompatible formats.

Remediate sensitive data incidents- either natively or through extensibility features (API, partner solutions, etc.)

Once sensitive data is reported by the proposed solution, action must be taken either manually, by college IT/IS staff or automatically, through an orchestrated response. The following questions will help us determine if remediation work can be done by the proposed solution, by API/proprietary partner integration, or manually by IT/IS staff after reporting (discussed in the previous section):

- ❑ Does your solution provide automated remediation? Please describe the capabilities, including those provided out-of-the-box if applicable.
- ❑ Does your solution require a software agent to be installed in order to perform remediation actions on a target server or endpoint?
- ❑ Please list what scripting languages could be automatically triggered by your software when an information match is found during a scan.
- ❑ What are the capabilities for customers to add their own automated remediation?
- ❑ Describe the solution’s ability to mark scanned files through metadata. These markings may be used by EDR or other endpoint/server software.

Simplify management of the solution through automation, intuitive interfaces, and scalable installation methods.

Limited IT staffing across the System necessitates solutions that can be efficiently managed. The Sensitive Data Discovery / DLP Solution should incorporate features that empower information technology and information security staff to find and triage sensitive data incidents while causing the least amount of interference and/or disturbance to business and IT operations. Below are requirements that will help us determine if your solution can be efficiently managed in the long term:

- ❑ Provide an easy-to-use GUI interface that enables proficiency without extensive training
- ❑ Please list the available deployment architectures for your proposed solution (cloud, hybrid, on-premise)
- ❑ Support VMWare ESXI and Nutanix AHV hypervisors, if virtual servers and/or appliances are required.
- ❑ Does your solution require an agent for any collection methods or are all collection methods supported without an agent? If so, how do agents communicate with your product: Is it a two-way communication, what ACLs/network ports need to be open to enable communication, what type of encryption is used to secure communication?
- ❑ Is the agent self-healing and updating after initial install? Please provide detail.
- ❑ Provide silent & automated installation methods that are compatible with endpoint management solutions (SCCM, Altiris, DesktopCentral, etc)

Align the solution with a multi-college distributed computing environment.

As stated in the Introduction/Background section, the MCCS is made up of the seven accredited community colleges across the state of Maine. Each college operates and maintains its own IT infrastructure. Recent initiatives have started to change this precedent by selecting and implementing shared systems that allow local control of a system but also creates opportunities for collaboration between colleges: Mainly knowledge sharing, creative problem solving, and depth of expertise.

The Sensitive Data Discovery / DLP Solution should align with this new direction. Multi-tenant solutions where colleges have their own space to operate but certain features are visible in an ‘enterprise view’ are well suited to our organizational structure. In the absence of ‘enterprise’ features, granular permissions and support for multiple identity providers / AD domains are a valid substitute. Outside of these two architectures, an ‘instance’ per college is another way to achieve separation while also maintaining one solution for the entire System. Below are requirements that will help us determine if your solution matches our organizational structure:

- ❑ Are there enterprise features that align with a federated organizational structure? I.e. parent/child company relationships, acquisitions / mergers, separation between entities.
- ❑ Does your solution support integration with multiple identity providers?
- ❑ Are there mechanisms to separate devices, scans, users, and results into organizational units?
- ❑ Describe user & group permissions, and the level of granularity that could support dozens of IT/IS employees using a system from 7 colleges & the system office.

- □ Does your solution provide a way to audit and record user activities?
- □ Describe how the solution supports multiple campus networks, including satellite locations that may or may not use a VPN, and employees working at home.

Support the solution through a variety of communication methods and knowledge sources.

Once the solution has been implemented and turned over to MCCS IT staff for operational use, a support structure should remain for questions and/or problems that manifest as PII is discovered and data regulations change. This support structure should be highly available, customer engaged, and go above and beyond to ensure the SDD / DLP solution continues to protect the MCCS from unauthorized data disclosures. The following questions / requirements will help us determine if there is an adequate support structure for the proposed SDD / DLP solution:

- □ What support options are available?
- □ Please describe your SLAs for support.
- □ Are support representatives responsible for more than one product? Please list all products supported by your support representatives.
- □ How often do you release updates or upgrades to your platform?
- □ How are customers notified about these upgrades?
- □ How do we receive updates to your platform when there are changes in compliance regulations or new products on the market which may be utilized within our organization?
- □ On average, how many levels of support does an end user need to navigate through before reaching someone directly familiar with your product?
- □ Are your product specific support teams located in the countries or regions where your customers are located? Please describe the locations of these product specific support personnel.
- □ Are any of your support personnel located in the same facilities as your product specific engineering personnel? If not, please explain the process by which your support personnel have access to engineering resources for advanced problem/issue resolution.
- □ What method do you employ to collect customer feedback and incorporate it into future releases?

6.2 Security

See Attachment A for a matrix to assist with providing the following information:

6.2.1 Requested Documentation
6.2.2 Information Security
6.2.3 Security Architecture
6.2.4 Facility Security
6.2.5 Resiliency
6.2.6 Compliance
6.2.7 Data Governance

Alternatively, an EDUCAUSE HECVAT report may be returned in lieu of answering questions in Attachment A.

6.3 Special Considerations

The MCCS is comprised of seven independently accredited community colleges, each with their own individual Student Information System (Jenzabar EX/J1), each with their own curriculum, and each their own student and employee identity and access authentication systems. Our EDR platform and shared LMS are early endeavors into collaboration across colleges. Please describe in detail how your solution can support this environment and provide examples and case studies of any other similar system or district that is using your Sensitive Data Discovery / DLP Solution.

7.0 TRAINING PROPOSAL

The Training Proposal must include a comprehensive plan for:

7.1 Knowledge transfer and documentation covering the proposed solution, all necessary non-default configuration, maintenance tasks, and opportunities for expansion & integration
7.2 System management training for technical personnel
7.3 Future training opportunities for new hires or role changes (self-paced, instructor led, etc)
7.4 Knowledge base information to share with faculty, students, administration, and the college community

8.0 COST PROPOSAL

Include a complete cost proposal, separated out into the following five areas

8.1 Software and license costs for the initial and additional contract duration specified in section 1
8.2 Configuration and setup costs including hourly rates for professional services
8.3 Training costs for items specified in section 7
8.4 Software maintenance and technical support costs with options for 24/7 and 8/5
8.5 Optional peripheral systems, services and software packages

MCCS strongly prefers a solution based on employee full-time equivalency (FTE) counts. The following data is current as of October 2020:

College	Full Time Staff/Faculty	Adjunct Faculty + Part Time Staff
CMCC	125	131 + 1
EMCC	126	48 + 3
KVCC	98	65 + 3
NMCC	88	17 + 2
SMCC	244	277 + 1
System Office	45	0 + 5
WCCC	38	16 + 1
YCCC	56	72 + 1
Totals	**820**	**643**

9.0 Interpretation of Contract Documents

No oral interpretation will be provided to any bidder as to the meaning of the specifications or other contract documents. Every request for such interpretation shall be made in writing at least three (3) or more business days before the proposal due date and submitted to:

Scott Fortin
Chief Information Security Officer
Maine Community College System
323 State Street
Augusta, ME 04330

or via email at sfortin@mccs.me.edu

Any interpretation made to a bidder will be issued in the form of an addendum to the contract/bid documents which, if issued, shall be sent as promptly as practicable to all persons to whom the specifications have been issued. All such addenda shall become part of the contract/bid documents.

10.0 Taxation and Compliance

MCCS is an educational institution organized under the laws of the State of Maine, and so its purchase of goods is exempt from state, federal, and local sales and use taxes. The successful bidder agrees to comply with all applicable federal, state and local statutes, laws, codes, rules, regulations, ordinances and orders in the performance of the Contract.

11.0 Evaluation and Scoring

Each proposal will be scored using the following matrix:

Item	Percentage Possible
BUSINESS PROPOSAL	5%
TECHNICAL PROPOSAL	35%
SECURITY	10%
SPECIAL CONSIDERATION	10%
TRAINING PROPOSAL	20%
COST PROPOSAL	20%
TOTAL	100%

12.0 Terms and Conditions

Standard Terms and Conditions applicable to all MCCS Contracts are included in ATTACHMENT B– TERMS.

Attachment A – Security Questionnaire

MCCS Vendor Security Questionnaire

Cloud Services Solution - Vendor Information	MCCS reviews the IT security of all Cloud-based services that store, process, or transmit data that MCCS considers to be Sensitive or Restricted. Please provide the documentation requested below and complete the questionnaire. N/A	
Requested Documentation	**Document Titles**	**Comments**
In addition to completing the questionnaire below, the following documentation should be provided to MCCS (as applicable or available and under a nondisclosure agreement - NDA - as needed in support of this security review.)	Cloud Security Alliance Consensus Assessments Initiative Questionnaire (if Cloud service provider) A vulnerability, penetration, or ethical hack report prepared by a third party (not by the vendor) Any documentation that describes your technical and security infrastructure Data flow diagram (for college data processed by the application/service)	MCCS cannot validate and approve services or applications without supporting documentation. Please attach the requested documentation when returning the Security Questionnaire.

Information Security	Information Security Questions	Comments and Notes
Management Program	Please describe your Security Management Program or attach a copy. Does your organization follow a particular security standard such as ISO-27001, ISO-22307, CoBIT, HITRUST, etc. or do you have your own?	
Policy Reviews	Can you notify us when changes are made to your security policies or procedures?	
User Access Policy	Please describe your employee termination procedures.	
Encryption Key Management	Will our data be encrypted at rest? What algorithm?	
	Will our data be encrypted in transit, including between servers? What algorithm?	
	Do you have an encryption key management system? If so, please tell us about it?	
Vulnerability / Patch Management	Do you conduct vulnerability scans of the servers?	
	Do you conduct application vulnerability scans?	
	Please explain your patching policy, timeframes, and procedures.	
Antivirus / Malicious Software	Do you have anti-malware or virus protection programs installed? Which programs?	
	How often are your malware/virus protection programs updated? How regularly are complete scans scheduled?	
Incident Management	How will you alert your clients if their data may have been breached? Do you have a documented security incident response plan?	
	Can you incorporate client-specific needs into your incident response plan?	
	Can you outline for us what responsibilities are ours, and what are yours for an incident?	
Incident Reporting	What method do you use for log management?	
	Does your logging and monitoring method allow for isolation of an incident to specific tenants?	

Incident Response Legal Preparation	How do you incorporate a "chain of custody" into your incident response plan?	
	Please share your procedures for forensic data collection and analysis?	
	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for us?	
Asset Returns	Please share a copy of your Privacy Policy.	
Audit Tools Access	How do you restrict, log, and monitor access to your systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	
Source Code Access Restriction	Please describe your Source Code Analysis process.	
Security Architecture	**Security Architecture Questions**	**Comments and Notes**
User ID Credentials	Please describe your identity management system and any options that are available to your clients.	
	Does your system support both role-based and context-based access to the data?	
	Do you support two-factor authentication? If so, what options are available?	
Data Security / Integrity	Is your Data Security Architecture designed using an industry-standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS)	
Application Security	Do you utilize NIST 800-64 (Security Considerations in the System Development Life Cycle) as the guideline for application development? Or, do you use another standard application security development framework?	
	Do you utilize an automated source-code analysis tool to detect code security defects?	
Data Integrity	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	
Production / Nonproduction Environments	Do you provide clients with separate environments for production and test processes?	

Remote User Multifactor Authentication	Is multi-factor authentication available for remote user access?	
Segmentation	Are systems and network environments logically separated?	
	Are systems and network environments segmented to allow isolation of restricted data?	
Wireless Security	What procedures are in place that require secure encryption for authentication and transmission during wireless transmission?	
	Have vendor default passwords been changed?	
Shared Networks	How is access to systems with shared infrastructure restricted to only appropriate personnel?	
Equipment Identification	How does the information system identify and authenticate devices before establishing a network connection?	
Audit Logging / Intrusion Detection	Are file integrity (host) and network intrusion detection (IDS) tools implemented?	
	Are audit logs protected from modification?	
Mobile Code	How is mobile code monitored and controlled in your system?	
	Is all unauthorized mobile code prevented from executing?	

Facility Security	Facility Security Questions	Comments and Notes
Policy	What policies and procedures exist for providing physical safeguards of the systems and environment?	
Controlled Access Points	What physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) have been implemented?	
Secure Area Authorization	Where will the data be located? Backups? Alternate data center?	
Offsite Authorization	Are you able to alert us if the data is to be moved to a different location?	

Resiliency	Resiliency Questions	Comments and Notes
Business Continuity Planning	Please explain your backup strategy? Disaster Recovery plan? Business Continuity plan?	
Equipment Power Failures	What types of mechanisms and redundancies are implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	
Power / Telecommunications	Please share a data flow diagram of your systems as related to backups/mirrors/failovers?	

Compliance	Compliance Questions	Comments and Notes
Independent Audits	Please share your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third-party audit reports.	
	Do you conduct network penetration tests?	
	Do you conduct application penetration tests of your cloud infrastructure yearly or after any upgrade?	
	Please share your penetration test results.	
Third Party Audits	Are clients able to conduct their own vulnerability scans?	
Information System Regulatory Mapping	Do you have the capability to logically segment and recover data for a specific customer in the case of a failure or data loss?	
Risk Management	Is your organization insured by a 3rd party for losses?	

Data Governance	Data Governance Questions	Comments and Notes
Retention Policy	Do you have capabilities to enforce client data retention policies?	
Secure Disposal	Are you able to support secure deletion (ex. degaussing/cryptographic wiping) of archived data as determined by the client?	
	What happens to the data at the end of the contract?	
Nonproduction Data	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	
Information Leakage	Do you have controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment?	
	Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?	

Attachment B – MCCS Terms and Conditions

NOTICE TO VENDORS AND BIDDERS: STANDARD TERMS AND CONDITIONS APPLICABLE TO ALL MCCS CONTRACTS

The following standard contracting terms and conditions are incorporated and shall become a part of any final contract that will be awarded by any college or other operating unit of the Maine Community College System (collectively “MCCS”).

These terms and conditions derive from the public nature and limited resources of the MCCS.

MCCS DOES NOT AGREE TO:

1. Provide any defense, hold harmless or indemnity;
2. Waive any statutory or constitutional immunity;
3. Apply the law of a state other than Maine;
4. Procure types or amounts of insurance beyond those MCCS already maintains or waive any rights of subrogation;
5. Add any entity as an additional insured to MCCS policies of insurance;
6. Pay attorneys’ fees; costs, including collection costs; expenses or liquidated damages;
7. Promise confidentiality in a manner contrary to Maine’s Freedom of Access Act;
8. Permit an entity to change unilaterally any term or condition once the contract is signed;
9. Automatic renewals for term(s) greater than month-to-month;
10. Limitations on MCCS’ recovery of lawful damages incurred as a result of breach of the contract;
11. Limitation of the time period under which claims can be made or actions brought arising from the contract;
12. Vendor’s terms prevailing over MCCS’ standard terms and conditions, including addenda; and
13. Unilateral modifications to the contract by the vendor.

BY SUBMITTING A RESPONSE TO A REQUEST FOR PROPOSAL, BID OR OTHER OFFER TO DO BUSINESS WITH MCCS, YOUR ENTITY UNDERSTANDS AND AGREES THAT:

1. The above standard terms and conditions are thereby incorporated into any agreement entered into between MCCS and your entity; that such terms and condition shall control in the event of any conflict with such agreement; and that your entity will not propose or demand any contrary terms;
2. The above standard terms and conditions will govern the interpretation of such agreement notwithstanding the expression of any other term and/or condition to the contrary;
3. Your entity will not propose to any college or other operating unit of the MCCS any contractual documents of any kind that are not in at least 11-point black font on a white background and completely contained in one Word or PDF document, and that any references to terms and conditions, privacy policies or any other conditions referenced outside of the contract will not apply; and
4. Your entity will identify at the time of submission which, if any, portion or your submitted materials are entitled to “trade secret” exemption from disclosure under Maine’s Freedom of Access Act; that failure to so identify will authorize MCCS to conclude that no portions are so exempt; and that your entity will defend, indemnify and hold harmless MCCS in any and all legal actions that seek to compel MCCS to disclose under Maine’s Freedom of Access Act some or all of your submitted materials and/or contract, if any, executed between MCCS and your entity.