Maine Community College System
323 State Street
Augusta, ME 04330

Competitive Bid
Request For Proposal
This is NOT an order.

Endpoint Protection System

Issue Date:	**May 17, 2019**
Questions from Bidders Due On:	**May 31, 2019**
Response Due Date:	**by 4:00 pm EDT on June 7, 2019**
Return Proposal To:	**David Haskell** **Information Support Specialist III** **Maine Community College System** **323 State Street** **Augusta, ME 04330** **207.629.4029** **dhaskell@mccs.me.edu**

Contents

1.0 PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit proposals from qualified vendors for procurement of a new generation of Endpoint Protection Solution for all seven Maine Community Colleges and the System Office and acquisition of professional services to implement it.

1.1 Business Objectives

The proposed endpoint protection solutions must enable or assist the colleges and System Office in achieving the following business objectives (the order of the list doesn't reflect the importance or the priority of the objectives):

a. Supports the mission of the colleges.
   - CMCC – Central Maine Community College provides quality, accessible college education and lifelong learning opportunities by offering career and technical education; education for transfer to the baccalaureate level; and services to support economic development and community vitality.
   - EMCC – Eastern Maine Community College provides the highest quality post-secondary technical, career, and transfer education and serves as a dynamic community and economic development resource.
   - KVCC – Kennebec Valley Community College prepares students to achieve their educational, professional, and personal goals in a supportive environment through shared values of responsibility, integrity, and respect.
   - NMCC – Northern Maine Community College is committed to maintaining its tradition of providing high-quality career and transfer programs that lead to associate degrees, certificates, and specialized training necessary for an educated, skilled and adaptable workforce. Through its affordable programs of study, courses, and specialized training seminars, the College is a catalyst for economic growth and the development of human potential.
   - SMCC – SMCC transforms lives and communities through education and training. We welcome, prepare and inspire all to learn, succeed and lead.
   - WCCC – Washington County Community College serves as an educational, community, and economic development resource for Washington County and beyond by providing educational and workforce training opportunities with individualized attention to all who desire to gain technical skills, develop career specializations, engage in self-improvement, and/or prepare for transfer.
   - YCCC – York County Community College provides academic, career, and transfer programs while serving to advance cultural, economic, and workforce development in York County and the State of Maine.
b. Must be capable of supporting the colleges' current needs and be able to adapt to the colleges' future information security needs as the threat landscape evolves.
c. Provides a central management systems console at each college that monitors and manages each college's installed base and reports infections and other alerts as configured.
d. Provides an endpoint security platform that integrates and interoperates with other information security systems and tools (existing and future) to improve the colleges' overall information security posture and enable all facets of the colleges' business.
e. Prevents cyber breaches by preemptively blocking known and unknown ransomware, malware, exploits, and zero-day threats.
f. Provides administrative access that is role-based, allowing IT staff to have appropriate access based on their assigned role.
g. Enables and protects all users as they safely perform their daily business activities using web-based technologies and local resources without becoming a hindrance or negatively affecting user experience with the colleges' systems.
h. Must be able to seamlessly integrate within the colleges/IT business activities and practices and not require a major change to the existing college and IT operations.
i. Must improve endpoint security and enables the colleges to utilize internet-based information and services safely.

j. Provides excellent detection and protection services to the colleges' systems to improve the colleges' responsiveness to changing business conditions.
k. Improves the colleges' systems' security, availability, resiliency, and capacity without being cost prohibitive.
l. Provides the colleges with a deeper understanding of the granular usage of the system application visibility and control.
m. Adhere to the colleges' information security plans to ensure all security guidelines and standards are achieved.
n. Support the Maine Community College System's policies related to safe data handling, data security, and acceptable technology use.
o. Provides excellent and timely customer support service to authorized IT staff through multiple channels such as customer support portal, chat, and toll-free number, remote troubleshooting, and mobile support based in the United States.
p. Must minimize the number of personnel needed to administer and monitor the system. Might not be objectively measurable.

1.2 Solution Vision

To acquire a next-generation endpoint protection solution which delivers the business objectives outlined above and can be efficiently managed and monitored by a minimal number of IT staff to keep the colleges' systems secure in today's changing threat landscape.

The selected solution will be deployed and integrated into the college systems in multiple phases to prevent any disruption to the college business. The first phase which involves planning, installation, configuration, and deployment of the selected solution to a subset of college systems must be completed by a date arranged with the IT leadership at each college after the RFP is awarded.

The selected vendor is expected to have the overall responsibility for the successful deployment and operation of the selected endpoint protection solution. The following work/commitment is expected from the selected vendor:

a. Provides deployment assistance (i.e., planning, best practices, etc.) to the IT staff.
b. Configures the cloud-based and local administrative console to the colleges' requirements and specifications.
c. Timely resolve deployment and operational issues as they arise during and after the deployment.
d. Provides training and continuous knowledge transfer to the identified IT staff to improve the colleges' staff's understanding of its solution during the project rollout.
e. Integrates and interoperates with the existing and future information security tools and systems such as SIEM, NAC, Firewalls, IDS/IPS, and ServiceDesk systems.
f. Provides periodic functional and feature improvements to the solution and administrative console to increase the effectiveness of its solution.
g. Provides the professional services that are necessary to satisfy the requirements contained within this RFP.

The solution vision outlined above may evolve during the implementation period. The selected vendor is expected to adapt to these changes and provide the necessary support to complete the deployment of the proposed solution as required in this RFP.

In summary, the selected vendor will provide:

- A complete, advanced endpoint protection solution that is not solely dependent upon signatures for malware identification
- Professional services to accommodate a phased deployment, ongoing software updates (to local agents, local management console, and the cloud-based console)
- Training to the select IT staff, support, and integration services for the proposed solution.

The colleges require vendors to provide all-inclusive pricing that covers all expenses associated with the work activities and solution components mentioned above.

2.0 PROJECT BACKGROUND

The new endpoint protection solution chosen through this RFP will provide an additional layer of information security for the colleges' systems, set a new standard for the protection of the colleges' endpoints, and must interoperate with the existing and new information security systems to improve the colleges' information security posture.

The procured solution will be centrally managed by each college IT staff and deployed in phases to the colleges' endpoints to minimize the chances of adversely impacting instruction.

We intend to choose a system that provides the best price/performance ratio and partner(s) that will meet the colleges' requirements and demonstrate the ability to grow with use for many years to come.

2.1 Current Environment

At present, the seven colleges and system office are utilizing multiple solutions on the college-owned systems to protect these systems from known malware and viruses. These current solutions are somewhat effective against traditional malware and viruses, but it is becoming less effective against Ransomware and other forms of advanced threats such as Zero-Day threats and polymorphic viruses.

Each college has the following number of endpoints that will need protection:

College	**Desktops**	**Microsoft Servers**	**iOS Devices**	**Macs**	**Android**	**Linux**
CMCC	750	110	40		20	
EMCC	600	60				
KVCC	600	50	200	30	25	
NMCC	500	50	40		10	
SMCC	1500	125	100	100		
WCCC	350	40	25	1		15
YCCC	350	50	25	5	20	
System Office	50	15	30	8	3	
Totals	4700	500	460	144	78	15

(Please note that a college may elect not to cover all endpoints. The numbers below represent the projected total units, not guaranteed total.)

The colleges have varying levels of Information Technology staff to provide user and endpoint systems support.

3.0 SCHEDULE & DEADLINES

Event	**Date and time**
MCCS issues RFP	May 17, 2019
Questions from Bidders Due	May 31, 2019 – 4 PM EDT
RFP Due Date	June 7, 2019 – 4 PM EDT
Selected Vendor Presentations	June 24 – 25, 2019
Recommendation Submitted to Executive Committee	June 28, 2019 – 4 PM EST
Notification of Award	July 2, 2019
Contract Start Date	TBD

Implemntation	TBD by each college

4.0 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 whole.

5.0 SUBMISSION INSTRUCTIONS

5.1 Proposal Transmission

While hardcopy proposals are also accepted (note mailing address below), electronic submission through email is the preferred method of delivering your proposal.

- Email proposals are preferred and should be sent to dhaskell@mccs.me.edu
- The Email Subject line must read "MCCS EPS RFP Response"
- Hardcopy proposals are to be mailed to:

  David Haskell
  Information Systems Specialist III
  Maine Community College System
  323 State Street.
  Augusta, ME 04330

- The mailed/emailed proposal must be RECEIVED no later than 4 PM EST on June 7, 2019
- MCCS will acknowledge receipt of all proposals sent through email within one business day.
- MCCS will not send confirmation of receipt of hardcopy proposals. Therefore, it is strongly encouraged that all hardcopy proposals be sent with a delivery confirmation required from the carrier.
- 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.

5.2 Modification or Withdrawal of Offers

The bidder's authorized representative may withdraw or modify their proposal, before 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.

5.3 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.

5.4 References

Please provide references from three (3) peer Institutions of Higher Education as part of your response, including the following information:

- Institution Name
- Technology Contact: Name, phone number, and e-mail

By submitting this information, the bidder authorizes MCCS to contact these clients for purposes consistent with the review of their proposal.

5.5 Reference Site Visits

MCCS may request a site visit to a bidder's working support center to aid in the evaluation of the bidder's proposal. Site visits, if required, will be discussed in the technical proposal.

5.6 Evaluation Environment

Within the proposal, provide an evaluation environment that allows for the local installation of at least ten machines with a web-based and a local-based management console. The environment should include the following:

- A set of login credentials for administration and management of the test environment:
- The required URL for accessing the test environment and downloading software for local clients.
- Access to as many relevant tools and technologies, and features/functionality as possible as outlined in your proposal
- The ability for MCCS personnel to add and modify at least ten computers into the test environment
- Working reporting tools
- A complete listing of any features that are not technically or logistically able to be included in this test environment

Because of the centrality of this testing environment to the Systems' evaluation of all proposals, access may be provided as soon as is practicable and can precede the completed submission of the proposal.

5.7 Vendor Presentations

Vendors may be requested to provide an on-site 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 the week of June 17, 2019. These presentations will not be open to the public.

If special accommodations are required to attend a site visit, email David Haskell at dhaskell@mccs.me.edu no later than seven (7) days before the scheduled presentation.

5.8 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 based on 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.

5.9 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
- ❑ A section labeled BUSINESS PROPOSAL as described in Section 6
- ❑ A section labeled SOLUTION REQUIREMENT as described Section 7 with the following identified subsections:
  - FUNCTIONAL REQUIREMENTS as described in Section 7.1
  - TECHNICAL REQUIREMENTS as described in Section 7.2
  - DESIRED FEATURES as described in Section 7.3
- ❑ A section labeled IMPLEMENTATION REQUIREMENTS as described in Section 8
- ❑ A section labeled COST PROPOSAL

6.0 BUSINESS PROPOSAL

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

6.1 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.

6.2 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.

6.3 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.

6.4 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.

6.5 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.

6.6 Authorizing Document

Respondent personnel signing the Transmittal Letter of the proposal must be legally authorized by the organization to commit the organization contractually. This section shall contain proof of such authority. A copy of corporate bylaws or a corporate resolution adopted by the board of directors indicating this authority will fulfill this requirement.

6.6 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 the 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.

6.7 General Information

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

6.8 Experience Serving Higher Education Institutions

Each Respondent is asked to please provide a brief description of your company's experience in serving higher educational institutions.

6.9 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.

7.0 SOLUTION REQUIREMENTS

If the 24x7 technical support is not included in the vendor's proposal as part of the solution, the vendor is required to submit additional pricing for this service. Additionally, the college requires vendors to submit a chart showing the total cost of ownership over three years period.

All professional services work must be done under the supervision of a highly qualified, certified expert. The overall technical responsibility of the project is to be carried out by this expert. At project completion, this expert must provide and sign-off on the final document(s) to acknowledge the conformity of the work completed by the vendor.

If the solution is awarded to multiple vendors (i.e., bidding vendor and its reseller), the vendors are responsible for their part of the project including the solution's integration with the college's network and coordination with other vendors working in parallel.

Bidders are required to submit their responses as a comprehensive turnkey solution. Therefore, all submittals must bundle the proposed solution, vendor-provided training, and technical labor, in addition to delineating material and labor in an itemized list, as part of the vendor's proposal. Any information provided by the colleges for this project is strictly confidential and shall not be disclosed to third parties without the approval of the MCCS legal counsel.

The proposed solution(s) must address the technical requirements and design objectives delineated herein. The vendor is solely responsible for delivering a fully functional solution meeting the specifications described herein. If the vendor regards the technical specifications as insufficiently exacting, he will offer equipment that will achieve the collective goals. Functional requirements apply before specific technical requirements, and the overall system requirements apply before the requirements for single components. After the award of the contract, the awarded vendor (contractor) is responsible for any necessary item not brought to the attention of the college before the award to complete the project by the specifications & design objectives.

7.1 Functional Requirements

1. Must be able to protect colleges' systems from Zero-Day exploits & attacks and not to rely solely on signature-based detection and protection methods.
2. Must have a proven track record effectively preventing enterprise endpoint systems from all Malware, including Ransomware, Zero-Day threats, polymorphic viruses, and other types of advanced threats.
3. Must provide an intuitive allow and deny capability that is auditable and granular that can be applied to an endpoint, group of endpoints or system-wide.
4. Must accommodate the colleges' multiple sites, with a level of college-based centralized operations that involve Information Technology diverse workforce with different skill-sets and varying responsibilities.
5. Must remove or minimize the current endpoint protection workloads that are manually handled by IT staff.
6. Must be able to interoperate with future SIEM, IDS/IPS, and other information security systems to provide an additional level of protection through early threat detection and prevention.
7. Must provide sandbox functionality including the ability to leverage a cloud or on-premise sandbox where the EDR solution can detonate files and analyze their behavior
8. Must provide network protection including a host-based firewall that can monitor incoming/outgoing traffic for malicious activity, especially activity masked as normal DNS/HTTP traffic
9. Must provide URL filtering include the ability to receive URL/IP blacklists from reputable sources as well as static lists configured by administrators
10. Must provide browser integration including plugins that interoperate with modern web browsers to assist end users in making good browsing decisions
11. Must protect diverse digital assets, including Microsoft Windows and Apple OSX based desktops, laptops, tablets, mobile devices, and servers.
12. Must provide a consistent, functional, college-based centralized administrative interface that is intuitive and easy to navigate.
13. Must provide the capability to make the routine tasks easier to manage.
14. Must provide a secure, cloud-based console for a single point of administration.
15. The solution should be able to automate the endpoint protection by autonomously reprogramming and retuning itself using threat intelligence gained from the behavioral analysis, reputation, and machine learning.
16. Must not rely on resource-intensive detection and protection methods that can adversely affect the performance of installed devices.
17. Ability to fully protect and support the colleges' mobile endpoints that are disconnected from colleges' networks for an extended period.
18. Must provide flexible alert notification capability to alert IT staff about suspicious activities that may pose a security threat to the colleges' assets.

19. Should provide both canned and tailorable email reporting of system health and status on a daily/scheduled basis which can be emailed to designated individuals.
20. Must provide a REST API to communicate and interoperate with other college systems to automate information security operational workloads.
21. The solution's agent should have a minimum footprint and performance impact on college endpoints (should not noticeably impact the end user's computing experience during scanning or continuous protection).
22. The cloud-based administrative console should be scalable to accommodate all related college workloads and must be resilient enough to provide maximum uptime.
23. The vendor should provide 24x7 product support over multiple channels including web-chat, WebEx, as well as the traditional channels such as email and phone support.
24. The vendor is expected to provide timely support for project planning, deployment, problem resolution for the proposed solution.
25. The vendor is expected to perform knowledge transfer of all necessary operational matter to IT staff to ensure the colleges can effectively manage and maintain all ongoing operations of the procured solution to keep all assets secure.

7.2 Technical Requirements

1. Agent applications must protect the following endpoints:
   a All Windows desktop versions including 7, 8.1 and 10 operating system versions (32 & 64 BIT) including variations of service packs
   b Apple OSX based systems
   c Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019
   d iOS version 11 or higher and Android OS version 7 or higher (desired)
2. The vendor must list the minimum hardware and software requirements for its endpoint agent; specify supported browsers to manage its administrative console application and any other requirement that is necessary to manage the proposed endpoint protection solution.
3. Must be able to retain the cloud-based console logs for a minimum of six months.
4. The false positive threat identification should be less than 1% of the installed college endpoints at any given time (for example, if the endpoint agent is installed on 100 college endpoints, the false positives should be less than 1).
5. The cloud-based administrative console and local admin console should always be responsive and accessible from anywhere to provide secure access to manage the endpoint protection solution.
6. The endpoint protection agent should not cause performance degradation on the installed colleges' systems.
7. The administrative console should adhere to responsive design principles to accommodate diverse endpoints (laptops, tablets, and phones as applicable).
8. The proposed solution must provide the capability to export the collected information to on-premises systems for additional processing.
9. The solution's agent must be easy to deploy, re-deploy, and manage through its life-cycle.
10. The solution should provide both real-time and historical reporting capability that is intuitive and easy to use, and the results should be exportable in multiple formats.
11. Only relevant information should be presented to the authorized console user (i.e., security trimmed) based on the user's role in the system. However, the console administrator(s) should have ultimate access to the system and all its components.
12. The detected threat information should be communicated to the system administrators and designated IT staff in real-time.
13. The console should provide all summary statistics in its main landing page.
14. Statistics for a different type of threats should be simultaneously displayed in a real-time in the vendor's console.

15. Real-time threat statistics should be displayed in graphical and numerical forms.
16. The system should have an open reporting architecture that easy to share and export to other systems.
17. The solution should provide the capability to generate status reports for the monitored endpoints on a predefined schedule.
18. The management system should be able to email the scheduled reports to identified college staff.
19. Status reports should be generated in HTML format to be shared and made available on an Intranet.
20. The solution should provide standardized, customized, and ad hoc reporting of the protected endpoints in both a real-time and a date range basis.
21. The solution must provide reporting methods to meet the GDPR reporting requirements for cybersecurity events
22. Any changes or upgrades to the management console should be scheduled and approved by the colleges.
23. The administration console should be available to any authorized college staff on any device and anytime.
24. The college staff should be given different levels of access that is appropriate with their role in support of the system (such as viewing real-time incident information and statistics and resolving individual incidents) as opposed to system-wide functions (creating and modifying policies for the solution) that is associated with the administrator level access.
25. The solution should support minimum Transport Level Security version 1.2 (TLS) to provide secure connections.
26. Solution's web console should be capable of filtering and sorting events to show only security-related data that is relevant and requires immediate attention.
27. The centralized management console should facilitate a granular new agent deployment and control of remote workstations.
28. The proposed endpoint protection solution should not cause or introduce security vulnerabilities to the college system.

7.3 Desired Features:

1. Interoperate with Active Directory through ADFS to provide access to system functions in addition to the console's local security database.
2. Provide integrated, remote remedial workflow, EDR capability that removes or reduces manual staff intervention.
3. Provide extensive Role-Based-Access (RBAC) to the administrative console to IT staff to enable college staff to complete their workloads promptly.
4. Audit assistive features that can produce reports given a specific file, signature, or behavior and provide information on how many endpoints were infected, how fast the infection spread, and average time to remediation.
5. Able to replace the existing endpoint solution (Microsoft's System Center Endpoint Protection software) without any consequence or loss of capability.
6. Protect IoT devices, Apple IOS, and Android-based systems.
7. Protect from fileless malware.
8. Provide easy and intuitive global search capability that provides an intuitive drill-down interface to assist in the investigation of suspicious activities.
9. Prevent uninstall of endpoint protection agent from the college-owned devices by end-users who have elevated (high privileged) access on those systems.
10. Able to uninstall the endpoint agent from the installed systems through the management console.
11. Able to investigate and mitigate the potentially infected endpoints remotely.
12. Provide SMS notification capability to timely alert college staff about malware and security threats.
13. Provide extensive, interactive reporting with drill-down capability on captured incidents.
14. Provide extensive, full auditing capabilities for every step of the system workflows.
15. Integration with the colleges' service management system to be able to automate the creation of incident tickets.

8.0 IMPLEMENTATION REQUIREMENTS

The colleges require the selected vendor to provide best industry practices for the implementation and management of proposed systems. It is very important for vendors to understand the colleges' requirements and come up with a plan to fulfill the requirements stated in this RFP.

Selected vendor must provide knowledge transfer of all relevant information.
The following requirements are mandatory:

8.1 Testing, Staging and Deployment Schedule

1. Vendors are required to submit the complete project plan and action steps specifying execution items.
2. The vendor is required to provide product roadmap (coming features) and its associated delivery date.
3. The vendor must provide a summary of known outstanding issues with the current version of the proposed solution and expected resolutions.
4. Vendors must work in such a manner that the college business is not affected in any way.
5. It is the vendor's responsibility to successfully deploy and integrate the procured solution into the college systems (install, configure, and integrate where it is appropriate) as per college business schedule and requirements.
6. Configure the management console to provide required functionality outlined in this RFP.
7. Describe any monitoring tools or plug-ins (i.e., Nagios plug-ins) that is available to monitor the system.

8.2 Training and Support

Training

a. Provide certified manufacturer training for eight employees from the colleges and System Office to be trained to configure, operate, and maintain the proposed solution.
b. This formal classroom training must be on-site and cover all key concepts and specific to the proposed solution. Remote training may be substituted for in-person training at the discretion of each college IT Leader.

Support

a. Describe if, how, and from where you will provide 24 x 7 support and the time frame of guaranteed initial response time during the acceptance period. Preference will be given to those who provide support based in the United States.
b. Specify whether you can provide on-site support in case of an emergency.
c. Include a proposed Service Level Agreement (SLA) which contains support levels, priority levels, response times, and contact methods.

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 no later than May 31 and submitted to:

David Haskell
Information Support Specialist III
Maine Community College System Office
323 State Street
Augusta, ME 04330

or via email at dhaskell@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%
FUNCTIONAL REQUIREMENTS	25%
TECHNICAL REQUIREMENTS	25%
DESIRED FEATURES	5%
IMPLEMENTATION REQUIREMENTS	20%
COST PROPOSAL	20%
TOTAL	100%

12.0 TERMS AND CONDITIONS

Standard Terms and Conditions applicable to all MCCS Contracts are included EPS RFP ATTACHMENT A – TERMS.

ATTACHMENT A – PRICING TEMPLATE

Request for Proposal for Procurement of Endpoint Protection Solution and Accompanying Professional Services

PRICING PAGE

In addition to this Pricing Summary Page, vendors must submit **complete and itemized listings** of all proposed charges (i.e., equipment, parts, and materials; software, shipping; labor, installation, integration, and implementation; maintenance options; etc.). Systems proposed must be fully functional. The cost of any omissions will be the responsibility of the vendor.

Lump Sum Hardware Cost	**$**
Lump Sum Software Cost	**$**
Lump Sum Labor, Installation, Integration, Implementation, Testing, Training, and Other Costs	**$**
Grand Total	**$**

Annual Hardware and Software Maintenance Options (pricing to be held firm for at least three years):

24 x 7 x 4	**$**
24 x 7 x NBD	**$**
8 x 5 x NBD	**$**

Vendor Name: _____

ATTACHMENT B – CONTRACT TERMS AND CONDITIONS

NOTICE TO ALL BIDDERS REGARDING CONDITIONS ON BIDS

STANDARD TERMS AND CONDITIONS APPLICABLE TO ALL MAINE COMMUNITY COLLEGE SYSTEM CONTRACTS

The following Maine Community College System (MCCS) standard contracting terms and conditions are incorporated and shall become a part of any final contract that will be awarded by any college or another operating unit of MCCS. These terms and conditions derive from the public nature and limited resources of 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 or costs for any other entity;
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; and
9. automatic renewals for term(s) greater than month-to-month.

By submitting a response to a Request for Proposal, bid or other like offer to do business with MCCS, **YOUR ENTITY UNDERSTANDS AND AGREES THAT:**

1. The above standard terms and conditions are thereby incorporated either expressly or by reference to this notice into any agreement entered into between MCCS and your entity, 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 MCCS any contractual documents of any kind that are not in at least 11-point font and completely contained in one Word or PDF document, and that any references to terms; 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.