



**Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology**

Remote Hosting Policy

I. Statement

Establish requirements and responsibilities for hosting Maine State computer applications by external hosting vendors.

II. Purpose

It is important that the citizens and partners of Maine State Government receive a uniformly high level of service from external vendors. Should the quality of service provided by external vendors fall below contracted service level agreements, it may not only cause customer hardship, but it may also tarnish the electronic branding of the State of Maine. Moreover, should there be a security breach in a Maine State application hosted by an external vendor, there may also be additional legal and statutory ramifications, as well as adverse media coverage. For these reasons, the Chief Information Officer has adopted this Remote Hosting Policy.

III. Applicability

This policy applies to any and all Maine State computer applications hosted by any party other than the Maine State Government. More specifically, it covers remotely hosted applications containing data owned by the Executive Branch and semi-autonomous State agencies, as well as remotely hosted applications from other Maine State Government branches that traverse the State's wide area network.

IV. Responsibilities

A. HOSTING VENDORS: A Hosting Vendor shall

1. In the event of a security breach incident, notify the Contract Administrator within three hours of first knowledge.
2. Comply with the Maine Public Law 10 MRSA §1347 (Notice of Risk to Personal Data Act)¹.
3. Comply with audits for compliance as identified in the contract.
4. Comply with data ownership as defined in the contract.

¹ <http://www.mainelegislature.org/legis/statutes/10/title10sec1347-A.html>

5. Provide support for the agency in compliance with FOAA (Freedom of Access Act) requirements and incident investigations.

6. Ensure the following:

a. A secure hosting infrastructure of the utmost:

(i) Confidentiality (No unauthorized access)

(ii) Integrity (No tampering)

(iii) Authenticity (No impersonation)

b. Data in its custody should never be used, under any circumstances, for any purposes other than those agreed to in the hosting contract.

c. All hosts, servers and devices should have currently-supported and hardened operating systems, the latest anti-viral, anti-hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, should have the most aggressive intrusion-detection and firewall protection.

d. At a minimum, 99% scheduled uptime, excluding planned downtime for maintenance.

e. Adequate capacity to ensure prompt response to both data inquiry/lookup and data modification transactions, at all times.

f. All hardware and software components of the hosting infrastructure should be fully supported by their respective manufacturers at all times.

g. A conservative sunset and migration schedule for all hardware and software components, as recommended by their respective manufacturers, at all times.

h. Periodic backups. The minimum acceptable frequency is differential backup daily, and complete backup weekly.

i. An aggressive regimen of patch management. All critical patches for operating systems, databases, web services, etc, should be applied within three working days of release by their respective manufacturers.

j. Complete backup-restore and disaster recovery tests from the appropriate media, once per annum.

k. Comply with the Records Retention Schedule of the Contracting Agency, as relevant to the data being hosted remotely.

l. Agree to transfer the data in its custody to another Hosting Vendor at the end of the hosting contract. Comply with audit verification that all data has been transferred that is necessary for record retention, access logging and investigation or FOAA and that no data is retained once the transfer is complete and receipt and usability have been confirmed.

- m. Submission to scheduled and random security audits, including vulnerability assessments, of the hosting infrastructure and/or the application, to be conducted under the auspices of the Enterprise Information Security Officer.
 - n. Complete cooperation with the Enterprise Information Security Officer in the detection and remediation of any security vulnerability of the hosting infrastructure and/or the application.
 - o. Expeditious remediation of any verifiable, infrastructural negligence.
 - p. Complete compliance with all Federal and Maine laws, regulations, statutes, policies, standards, and best practices relevant to internet-based hosting.
7. Submit the following detailed reports. All reports should be submitted to the Contract Administrator. Unless otherwise stated, these reports should be filed initially at the inception of the contract, and subsequently, once per annum, as well as corresponding to every substantive change in the subject matter of the relevant report.
- a. Uptime and Unplanned Outage Report. This report should be submitted once per quarter.
 - b. Planned Downtime Notice. This notice should be submitted at least one week prior to the event.
 - c. Physical access controls for the hosting site.
 - d. Internal security awareness training curriculum and schedule. Should include the syllabus, the class schedule for new employees, annual refresher training, and any emergency, ad-hoc training.
 - e. Self-audit on software and hardware modifications, patches applied, etc. This report should be submitted at least twice per annum.
 - f. Backup-restore and disaster recovery procedures, and the results of the annual tests.
 - g. Security Breach Incident Reporting mechanism.
 - h. Production Change Management procedure.
 - i. Password Policy.
 - j. Event Logging & Auditing practices for Networks, Operating Systems, Applications, and Databases.
 - k. Installation/Configuration and Maintenance documentation.
 - l. Any other relevant, internal security-related standards, policies, procedures, best practices, etc, that govern the hosting infrastructure and/or the application, including, the

results of any third-party audits.

B. ENTERPRISE INFORMATION SECURITY OFFICER: The Enterprise Information Security Officer shall:

1. Direct scheduled and random security audits, including vulnerability assessments, to the hosting infrastructure and/or the application.
2. Coordinate the security auditing with the Technology Business Consultant (TBC) of the Contracting Agency and the Hosting Vendor, in case of scheduled audits.
3. Alert the TBC of the Contracting Agency should an information security deficiency be discovered, and subsequently recommend a remediation strategy. At her/his discretion, the Enterprise Information Security Officer may recommend the shutdown, or reduced operation, of the hosting infrastructure and/or the application, indefinitely.
4. Evaluate all notifications and submissions from the Hosting Vendor, and act upon them, as appropriate, including recommending the shutdown, or reduced operation, of the hosting infrastructure and/or the application, indefinitely.
5. Determine, in the event of a security vulnerability and/or an actual security breach, whether it was caused by infrastructural negligence on the part of the Hosting Vendor.

C. TECHNOLOGY BUSINESS CONSULTANT: The TBCs shall:

1. Assist the Enterprise Information Security Officer in the implementation of this Policy.
2. Ensure that the hosted application complies with the Application Deployment Certification Policy and the Website Acceptance Policy prior to its deployment.
3. Evaluate the business impact of a security breach incident notification from the Hosting Vendor, and liaise with the affected business stakeholders of the Contracting Agency.
4. Evaluate the business impacts of the Uptime and Unplanned Outage Report and the Planned Downtime Notice from the Hosting Vendor, and liaise with the affected business stakeholders of the Contracting Agency.

D. CONTRACT ADMINISTRATOR: The Contract Administrator shall

1. Ensure that all pertinent Requests for Proposals, and resulting Contracts with vendors, contain language in accord with this Policy, and attendant standards, operating procedures and best practices.
2. Ensure that all pertinent Requests for Proposals, and resulting Contracts with vendors, contain language in accord with the Records Retention Schedule of the Contracting Agency, as relevant to the data being hosted remotely.
3. Act as the negotiator between the Enterprise Information Security Officer and the TBC of the Contracting Agency on the one hand, and the Hosting Vendor on the other hand. Convey all communication from the Hosting Vendor to the Enterprise Information Security Officer and the TBC of the Contracting Agency, and *vice-versa*.

4. Instruct this Hosting Vendor to transfer the data in its custody to another Hosting Vendor at the end of the hosting contract.

E. **CONTRACTING AGENCY:** The Contracting Agency shall

1. Provide requirements in the contract that meet State of Maine Laws and Policy.
2. Explicitly state the data ownership in the contract.
3. Explicitly provide for audits for compliance and verification in the contract.
4. Explicitly provide for FOAA (Freedom of Access Act) and investigation requirements in the contract. These may cover logging of access to the data in addition to the data itself.

V. **Directives**

A. Complete and exclusive ownership of the hosted data rests with the Contracting Agency, and is not subject to any conditions.

B. The remediation costs for any security vulnerability and/or an actual security breach, that unambiguously results from verifiable, infrastructural negligence on the part of the Hosting Vendor, shall be borne entirely by the Hosting Vendor. In addition to the contents of this Policy, current computer security industry best practices, as defined by premier computer security industry guilds and consortiums, will be used to determine as to what constitutes infrastructural negligence on the part of the Hosting Vendor. The Enterprise Information Security Officer shall remain the final arbiter in this matter.

C. The remediation of a security vulnerability and/or an actual security breach in the application proper, as opposed to the underlying infrastructure, is considered an enhancement to the application, and should be pursued by the Contracting Agency outside the scope of this Policy.

D. The Maine Office of Information Technology will propose, adopt and implement standards, operating procedures and best practices in support of this Policy.

VI. **Definitions**

1. **APPLICATION:** A subclass of computer software that produces results of direct value to its users. The Application is contrasted with system software that manages a computer's internal functions but does not deliver any result of direct value to its users.
2. **TBC:** For the purpose of this Policy, the term TBC is construed to mean not just the Technology Business Consultants in the Executive Branch of Maine State Government, but also their analogous counterparts in the Legislative and Judicial Branches and Constitutional Officers, who provide technical leadership and customer liaison in their respective agencies and departments.
3. **INFRASTRUCTURE:** Encompasses all aspects of information technology other than the Applications proper. It consists of devices, networks, servers, operating systems, databases, webservers, firewalls, intrusion detection, etc.

4. **HOSTING VENDOR:** A commercial entity, external to the Maine State Government, that hosts a Maine State computer application. The Hosting Vendor is contrasted with the Application Vendor, ie, a commercial entity that creates a Maine State computer application.
5. **CONTRACT ADMINISTRATOR:** The officer of the State of Maine agency or department that is the signatory to the remote hosting contract with the Hosting Vendor.
6. **CONTRACTING AGENCY:** The State of Maine agency or department whose business is being served by the remote hosting contract with the Hosting Vendor.

VII. References

1. [Application Deployment Certification Policy](#)²
2. [FOAA \(Freedom of Access Act\)](#)³
3. [Website Acceptance Policy](#)⁴
4. [Technology Vulnerability Assessments Policy](#)⁵

VIII. Document Information

Adoption Date: January 8, 2007
Effective Date: January 8, 2007
Update Date: July 31, 2013
Next Review Date: July 31, 2015

Point of Contact: B. Victor Chakravarty, Enterprise Architect, Office of Information Technology, 207-624-9840.

Approved By: James R. Smith, Chief Information Officer, Office of Information Technology, 207-624-7568.

Position Title(s) or Agency Responsible for Enforcement: Dan Durgin, Enterprise Information Security Officer, Office of Information Technology, 207-624-9811.

Legal Citation:

Waiver Process: See the [Waiver Policy](#)⁶.

² <http://www.maine.gov/oit/policies/AppDeployCert.htm>

³ <http://www.maine.gov/oit/policies/FOAAPolicy2.htm>

⁴ <http://www.maine.gov/oit/policies/WebsiteAcceptancePolicy.htm>

⁵ <http://www.maine.gov/oit/policies/VulnerabilityAssessmentFinal.htm>

⁶ <http://maine.gov/oit/policies/waiver.htm>