



Maine State Government  
Dept. of Administrative & Financial Services  
Office of Information Technology (OIT)

## Remote Hosting Policy

### I. Statement

Establish requirements and responsibilities for remote-hosted Maine State computer applications.

### II. Purpose

Maine State Government expects all remote-hosted environments to be secure, reliable, and to utilize fully-supported infrastructure. This is critical due to the potential stakeholder hardship, State of Maine branding impact, legal and statutory ramifications, and adverse media coverage resulting from a security breach or service-quality issue. For these reasons, the Chief Information Officer has adopted this Remote Hosting Policy.

### III. Applicability

This policy applies to all Maine State Executive Branch remote-hosted information assets and any remote-hosted information assets (regardless of the Branch) utilizing the State wide area network. For policy purposes, OIT-Housing is considered Remote Hosting. Consumer-grade mass-market applications are exempt (such as DropBox, Quickbase, etc.)

### IV. Responsibilities

#### A. Hosting Vendors:

1. Notify Contract Administrator within three hours of first knowledge of a security breach.
2. Comply with Maine Public Law [Title 10, Chapter 210-B: NOTICE OF RISK TO PERSONAL DATA](#)<sup>1</sup>.
3. Fulfill all compliance audits identified in the contract.
4. Comply with data ownership as defined in the contract.
5. Provide support with [Freedom of Access Act \(FOAA\)](#)<sup>2</sup> requests and incident investigations.
6. The Cyber Liability of the Remote Hosting vendor is a function of the service that is actually being consumed. More specifically, the vendor is liable for any cyber security

---

<sup>1</sup> <http://www.mainelegislature.org/legis/statutes/10/title10ch210-bsec0.html>

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

## Remote Hosting Policy

vulnerability in the actually consumed services. Thus, for SaaS, the entire cyber liability is borne by the vendor. For PaaS, the vendor's cyber liability is limited to the Development and/or Deployment framework actually being consumed. For IaaS, the vendor's cyber liability is limited to the computing infrastructure, such as Processor, Storage, Operating System, etc., actually being consumed.

### 7. 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. All hosts, servers and devices have currently-supported and hardened operating systems, the latest anti-malware utilities and have the most aggressive intrusion-detection and firewall protection.

c. All hosting infrastructure hardware and software components are fully supported by their respective manufacturers, at all times.

d. An aggressive regimen of patch management. All critical patches for operating systems, databases, web services, commodity applications, etc., are tested prior to deployment and are applied within two weeks of release by their respective manufacturers.

e. A sunset and migration plan for all hardware and software, in alignment with the respective manufacturers' published best practices.

f. A minimum of 99% scheduled uptime, excluding planned downtime for maintenance.

g. A Disaster Recovery site with all the capabilities of the Primary site; utilizing a completely independent infrastructure stack and geographically separated by a minimum of one hundred miles from the Primary site. Both sites must be within the Continental United States.

h. A full Disaster Recovery exercise within one year of project go-live, repeated annually thereafter, and signed off by the Agency. This includes complete backup-restore tests from the appropriate medium once per annum. This exercise needs to be coordinated / scheduled with the Contract Administrator.

i. Periodic backups occur on a regularly scheduled basis. Backup frequency and backup retention are based on Contracting Agency needs for ensuring business continuity and data integrity. The minimum acceptable backup frequency is differential backup daily, and complete backup weekly.

j. Hosting infrastructure complies with the highest industry standards of data security for any remote hosted contents that include Personally Identifiable Information (PII). At the

## Remote Hosting Policy

least, the data center must be certified to [SSAE 16 SOC 2 Type II](https://www.ssae-16.com/category/ssae-16-type-ii/)<sup>3</sup>. It is preferred that the data center be certified to [FISMA Level 3 ATO](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)<sup>4</sup> and/or [FedRAMP CSP](http://cloud.cio.gov/fedramp/csp)<sup>5</sup>. Any device that stores PII or other High-Risk data must be statically encrypted to AES-256 strength. Any transmission of PII or other High-Risk data must be encrypted to at least TLS 1.0 strength

k. Data in its custody is never used for any purposes other than those agreed to in the hosting contract.

l. Data residency remains in the Continental United States at all times.

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

n. Compliance with Records Management requests. Full compliance with the Records Retention Schedule of the Contracting Agency occurs as relevant to the data being hosted remotely. This shall be minimally in accordance with the [Maine State Archivist Records Management General Schedule](http://maine.gov/sos/arc/records/state/gensched2.html)<sup>6</sup>

o. Upon termination of the contract all Agency data must be transferred to another Hosting Vendor. Compliance 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.

p. Full, timely participation in scheduled and random security audits, including hosting infrastructure and/or the application vulnerability assessments, conducted under the auspices of the Office of Information Technology's Enterprise Security Officer (ESO).

q. Complete cooperation with the ESO in the detection and remediation of any hosting infrastructure and/or the application security vulnerability.

r. Expeditious remediation of any infrastructural negligence that is verifiable.

s. Complete compliance with all Federal and Maine laws, regulations, statutes, policies, standards, and best practices relevant to internet-based hosting.

8. Submit the following detailed reports to the Contract Administrator. Unless otherwise noted below, reports should be filed at contract inception, 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: Should be submitted once per quarter.

b. Planned Downtime Notice: Should be submitted at least two weeks prior to the event.

---

<sup>3</sup> <https://www.ssae-16.com/category/ssae-16-type-ii/>

<sup>4</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<sup>5</sup> <http://cloud.cio.gov/fedramp/csp>

<sup>6</sup> <http://maine.gov/sos/arc/records/state/gensched2.html>

## Remote Hosting Policy

- c. Physical access controls for the hosting site.
- d. Internal security awareness training curriculum and schedule. Include the syllabus, new employee class schedule, annual refresher training, and any emergency, ad-hoc training.
- e. Self-audit on all 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 any associated test results. This includes results from the annual Disaster Recovery exercise.
- g. Security Breach Incident Reporting mechanism.
- h. Production Change Management procedure, Password Policy, and any relevant, internal security-related standards, policies, procedures, best practices, etc., that govern the hosting infrastructure and/or application, including any third-party audit results.
- i. Event Logging & Auditing practices for Networks, Operating Systems, Applications, and Databases.
- j. Any up-to-date third party security audit reports such as:
  - SSAE 16 SOC 2 Type II
  - FISMA Level 3 ATO
  - FedRAMP CSP
  - ISO/IEC 27001:2005
  - US-EU Safe Harbor Framework
  - SkyHigh CloudTrust
  - PCI-DSS

Based on up-to-date third party audit reports; the Contract Administrator *may* relieve the hosting vendor from some of the reporting requirements enumerated above.

### B. Technology Business Consultants (TBCs) and Application Directors (joint responsibility):

1. Assist the Enterprise Security Officer (ESO) in the implementation of this Policy.
2. Ensure that the hosted information asset complies with relevant deployment certification ([Application Deployment Certification Policy](#)<sup>7</sup>) 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 Planned

---

<sup>7</sup> <http://maine.gov/oit/policies/Application-Deployment-Certification.htm>

## Remote Hosting Policy

Downtime Notice Report from the Hosting Vendor, and liaise with affected business stakeholders.

### C. Enterprise Security Officer (ESO):

1. Direct scheduled and random security audits, including vulnerability assessments, to the hosting infrastructure and/or the application.
2. Coordinate security audits with the Contract Administrator, TBC, Application Director and the Hosting Vendor.
3. Alert the Contract Administrator, TBC and Application Director of any discovered security deficiency, and subsequently recommend a remediation strategy. At her/his discretion, the ESO may recommend the shutdown, or reduced operation, of the hosting infrastructure and/or the application, indefinitely.
4. 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.

### D. Contract Administrator:

1. Ensure pertinent Requests for Proposals (RFPs), and resulting Contracts, contain language in accord with this Policy, and attendant standards, operating procedures, and best practices.
2. Ensure pertinent RFPs, and resulting Contracts, contain language in accord with the Records Retention Schedule of the Contracting Agency, as relevant to the remote hosted data, and any other relevant State of Maine Laws and Policies.
3. Act as the facilitator between the ESO/TBC/Application Director and the Hosting Vendor. Convey all communication between the Hosting Vendor and the ESO/TBC/Application Director. Vets detailed reports from the hosting vendors with appropriate technical resources.
4. Instruct this Hosting Vendor to transfer the data in its custody to another Hosting Vendor at the end of the hosting contract.
5. Explicitly state the data ownership in the contract.
6. Explicitly provide for audits for compliance and verification in the contract.
7. Explicitly provide for FOAA (Freedom of Access Act) and investigation requirements in the contract. This includes not only access to the data itself, but system log information regarding the data access.

### V. Directives

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

## Remote Hosting Policy

B. The Hosting Vendor shall fully bear remediation costs for any security vulnerability and/or security breach that unambiguously results from verifiable Hosting Vendor negligence. In addition to this Policy, current computer security industry best practices, defined by premier computer security industry guilds and consortiums (such as [SANS.org](http://www.sans.org)<sup>8</sup>); will be used to determine what constitutes Hosting Vendor infrastructural negligence. The ESO is the final arbiter in this matter.

### VI. Definitions

1. Application Director: Provides oversight to multiple application development/support teams.
2. Contract Administrator: Identified in Rider B/B-IT of the remote hosting contract. In some cases, the Information Technology (IT) Manager may perform the Contract Administrator duties identified in this document.
3. Hosting Vendor: Commercial external entity that hosts Maine State information assets.
4. Infrastructure as a Service (IaaS): Computing infrastructure, such as Processor, Storage, Operating System, etc. consumed from the Cloud
5. OIT-Housing – equipment that resides in an OIT data center, where OIT provides only the physical security, uninterrupted electricity, climate control, rack space, and Internet connectivity. The hosting vendor provides everything else.
6. Personally Identifiable Information (PII): Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Refer to [Maine Public Law 10 MRSA § 1347](#)<sup>9</sup> for a more detailed definition. PII includes, but is not limited to Protected Health Information (PHI), Federal Tax Information (FTI), and Federal Education Rights and Privacy Act (FERPA) Information.
7. Platform as a Service (PaaS): Development and/or Deployment framework consumed from the Cloud
8. Software as a Service (SaaS): End-user application consumed from the Cloud.
9. Stakeholder: Any party potentially impacted by the change.
10. Technology Business Consultant: Agency information technology customer liaison.

### VII. References

### VIII. Document Information

---

<sup>8</sup> <http://www.sans.org/>

<sup>9</sup> <http://www.mainelegislature.org/legis/statutes/10/title10sec1347-A.html>

## Remote Hosting Policy

Initial Issue Date: January 8, 2007

Latest Revision Date: October 7, 2014

Point of Contact: Henry Quintal, Architecture-Policy Administrator, OIT, 207-624-8836.

Approved By: James R. Smith, Chief Information Officer, OIT, 207-624-7568

Position Title(s) or Agency Responsible for Enforcement: Enterprise Security Officer, OIT, 207-624-7568.

Legal Citation: 5 M.R.S.A. Chapter 163 Section 1973 paragraphs (1) B and (1) D, which read in part, “The Chief Information Officer shall:” “Set policies and standards for the implementation and use of information and telecommunications technologies...” and “Identify and implement information technology best business practices and project management.”

Waiver Process: See the [Waiver Policy](#)<sup>10</sup>.

---

<sup>10</sup> <http://maine.gov/oit/policies/waiver.htm>