Maine State Government
Department of Administrative and Financial Services
Office of Information Technology

Remote/Cloud Hosting Policy

1.0. Purpose

Maine State Government expects all Remote/Cloud-hosted information assets to be secure and reliable. Any service degradation, or information leak, in a Remote/Cloud-hosted information asset, will likely cause stakeholder hardship, reputational damage, and adverse legal and statutory ramifications. For these reasons, this Policy establishes requirements and responsibilities for Remote/Cloud-hosted information assets.

2.0. Definitions

2.1. *Agency Contract Administrator:* Explicitly identified in the contract as the Point-of-Contact representing the State of Maine Government (most likely, the specific Agency) vis-à-vis the CSP.

2.2. *Cloud Service Provider (CSP):* External entity that hosts a Maine State Information Asset, according to a contract.

2.3. *Commodity Cloud Application:* An application that is consumed from the Internet, exclusively based on a (most likely non-negotiable) End-User License Agreement (EULA) or Terms of Service, i.e., without a dedicated and/or negotiated purchasing contract. The application could be either free, or incur a usage fee. Example: Intuit QuickBooks.

2.4. *Information Asset:* Used interchangeably with Information System. Any discrete, identifiable piece of information technology, including hardware, software, and firmware.

2.5. *Information Assurance:* Measures that protect and defend information and information systems, by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

2.6. *Infrastructure as a Service (IaaS):* Computing infrastructure, such as Processor, Storage, Operating System, Hypervisor, etc. consumed from the Cloud. The more detailed NIST definition:[1] "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)."

2.7. *OIT Housing:* Equipment that resides in an OIT data center, where OIT provides the physical security, uninterrupted electricity, climate control, rack space, and Internet connectivity, including network segmentation. The OIT Housing Vendor provides *everything else*.

2.8. *Personally Identifiable Information (PII):* Information that can be used on its own, or in combination with other information, to identify, contact, or locate a single person, or to identify an individual in context. Refer to Paragraph 6 of Maine Public Law 10 MRSA § 1347[2] 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.

2.9. *Platform as a Service (PaaS):* Development and/or Deployment framework consumed from the Cloud. The more detailed NIST definition:[3] "The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources."

2.10. *Software as a Service (SaaS):* End-user application consumed from the Cloud. The more detailed NIST definition:[4] "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure . The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[2] http://www.mainelegislature.org/legis/statutes/10/title10sec1347.html
[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[4] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3.0. Applicability

3.1. This policy applies to:

3.1.1. All State of Maine Executive Branch information assets not under OIT hosting. This includes both general-purpose public cloud vendors, as well has narrower, vendor-specific, proprietary hosting offerings. This policy does not make any distinction between these two flavors, and all provisions of this policy apply uniformly across both flavors.

3.1.2. OIT-Housing, as a special case of Remote/Cloud Hosting.

3.1.3. Commodity Cloud Applications are *exempt* from this Policy. For further details, see the User Device and Commodity Application Policy.[5]

4.0. Responsibilities

4.1. Chief Information Security Officer (CISO):

4.1.1. Assists the Agency Contract Administrator in the enforcement of this Policy.

4.1.2. Directs scheduled and random security audits, including vulnerability and compliance assessments, of the Remote/Cloud-hosted information assets.

4.1.3. Coordinates audits with the Agency Contract Administrator, the OIT Information Asset Owner, the Account Manager, and the CSP, for external audit compliance.

4.1.4. Alerts the Agency Contract Administrator, the OIT Information Asset Owner, the Account Manager, and the CSP, of any discovered security deficiency, and subsequently recommends a remediation strategy. At their discretion, the CISO (in consultation with the Chief Information Officer) may order the shutdown, or reduced operation, of the Remote/Cloud-hosted information assets.

4.1.5. Determines, in the event of a security vulnerability, and/or an actual security breach, whether it was caused by negligence on the part of the CSP.

4.2. Cloud Service Provider (CSP):

4.2.1. Unless otherwise specified in the contract, or demanded by regulatory compliance, in the event of a breach of security, or suspected security incident, intrusion, leakage, unauthorized use, or disclosure involving confidential information, the CSP must notify OIT by a telephone call (207-624-7700), and email to OIT Information Security (Security.Infrastructure@maine.gov), within the following timeframes:

4.2.1.1. Upon the discovery of a breach of security, or suspected security incident or leakage, involving confidential information in electronic, or any other medium, if the information was, or is reasonably believed to have been, acquired by an unauthorized person; or

4.2.1.2. Within twenty-four (24) hours of the discovery of any suspected security incident, leakage, intrusion, unauthorized use, or disclosure of confidential information, or potential loss of confidential information.

[5] https://www.maine.gov/oit/policies/UserDeviceCommodityAppPolicy.pdf

4.2.2. Maintains compliance with all Federal and Maine laws, regulations, statutes, and rules, relevant to Remote-hosting (Cloud), including, but not limited to:
- 4.2.2.1. Maine Public Law Title 10, Chapter 210-B: NOTICE OF RISK TO PERSONAL DATA,[6] and any other pertinent Federal/State legal regulations regarding personal data.
- 4.2.2.2. All relevant OIT Policies, Standards, and Procedures.[7]
- 4.2.2.3. The Records Retention Schedule, in accordance with the Maine State Archivist Records Management General Schedule.[8]
- 4.2.2.4. Freedom of Access Act (FOAA)[9] requests and investigation requirements. This pertains to not only the data itself, but system log information as well.

4.2.3. Fulfills all contractual obligations, including:
- 4.2.3.1. Protection of sensitive information.
- 4.2.3.2. Discovery and Notification of breach of sensitive information.
- 4.2.3.3. Notification to individuals.
- 4.2.3.4. Use restriction.
- 4.2.3.5. Certification of return of sensitive information and tangible property at the end of the contract.
- 4.2.3.6. All accounting, records, and audit compliance requirements, commensurate with the data being transacted, and its specific oversight stipulations.
- 4.2.3.7. All data ownership directives.
- 4.2.3.8. All data residency directives.
- 4.2.3.9. All data handling and transfer directives.
- 4.2.3.10. All Cyber Liability directives.
- 4.2.3.11. Scheduled Uptime requirements. Unless otherwise specified in the Contract, by default, 99.9% scheduled uptime, excluding planned downtime for maintenance, is required.
- 4.2.3.12. Adequate capacity to meet the performance/response time requirements defined in the Contract, for both data inquiry/lookup, and data modification transactions.
- 4.2.3.13. Business Continuity and Disaster Recovery plans meet or exceed the Recovery Time Objectives (RTO) and the Recovery Point Objectives (RPO) defined in the Contract.

4.2.4. Provides a Hosting Environment that:
- 4.2.4.1. Is secure, and of the utmost:
  - 4.2.4.1.1. Confidentiality (No unauthorized access);
  - 4.2.4.1.2. Integrity (No tampering); and
  - 4.2.4.1.3. Availability (Reliable access).
- 4.2.4.2. Has Components that:

[6] http://www.mainelegislature.org/legis/statutes/10/title10ch210-bsec0.html
[7] https://www.maine.gov/oit/policies
[8] http://www.maine.gov/sos/arc/records/state/generalschedules.html
[9] http://www.maine.gov/oit/policies/FOAAPolicy.pdf

4.2.4.2.1. Are fully hardened, as recommended by the original product vendors (or other accountable parties).
4.2.4.2.2. Are fully supported by the original product vendors (or other accountable parties). This includes "Extended Support", not just "Service Pack" or "Mainstream Support."
4.2.4.2.3. Are fully patched, as recommended by the original product vendors (or other accountable parties), and the patches are tested in a non-production environment prior to deployment.
4.2.4.2.4. Utilize the latest anti-malware, data loss protection, and intrusion detection/protection, all from the respective Gartner Leader quadrants.
4.2.4.2.5. Utilize an end-of-life sunset and migration plan, as recommended by the original product vendors (or other accountable parties).
4.2.4.2.6. Are physically located within the Continental United States.[10]
4.2.4.2.7. Does not contain any Component blacklisted by any arm of the U.S. Federal Government.

4.2.5. Provides a Disaster Recovery site that:
4.2.5.1. Contains all the capabilities of the Primary site.
4.2.5.2. Utilizes a completely independent infrastructure stack.
4.2.5.3. Is geographically separated by a minimum of one hundred miles from the Primary site.
4.2.5.4. Is physically located within the Continental United States.

4.2.6. Conducts:
4.2.6.1. A full Disaster Recovery exercise within one year of go-live, and repeated annually thereafter, and signed off by the Agency Contract Administrator. This includes complete backup-restore tests from the appropriate medium once per year. This exercise must be coordinated with the Agency Contract Administrator.
4.2.6.2. Periodic backups on a regularly scheduled basis, with backup frequency and backup retention based on the State of Maine requirements for ensuring business continuity and data integrity, that meet or exceed the defined RTO and RPO. The minimum acceptable backup frequency is differential backup daily, and complete backup weekly. Backups must be stored in a different, geographically diverse, and secure location.

4.2.7. Guarantees the following regarding any data in its custody:
4.2.7.1. Any data other than Public Data (TLP: White) must be encrypted both at rest (AES 256), and in transit (Per NIST 800-52,[11] the minimum acceptable level of dynamic encryption is TLS 1.2).

[10] https://www.usgs.gov/faqs/what-constitutes-united-states-what-are-official-definitions
[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

4.2.7.2. Data is never used for any purposes other than those agreed to in the Contract.
4.2.7.3. Any CSP personnel (employee or contractor) with access to the data must have successfully passed an FBI fingerprint-based background check, signed a Non-Disclosure Agreement, and successfully completed the CSP's Security Awareness Training.
4.2.7.4. Ensures that appropriate access controls, and separation of duties, exist amongst the CSP personnel.

4.2.8. Participates, in a full and timely manner, in any scheduled and random security audit, including vulnerability and compliance assessments, requested by either the Agency Contract Administrator and/or the CISO, and/or required for external audit compliance.
4.2.8.1. Provides complete cooperation with the State of Maine in the detection and remediation of any vulnerability or deficiency.
4.2.8.2. Performs expeditious remediation of any verifiable vulnerability or deficiency.

4.2.9. Submits the following detailed reports to the Agency Contract Administrator. Unless otherwise specified, reports must be filed at contract inception, and annually thereafter, or when a substantive change transpires in the underlying subject matter of the report.
4.2.9.1. Uptime and Unplanned Outage Report: Once per quarter.
4.2.9.2. Planned Downtime Notice: At least two weeks prior to the event.
4.2.9.3. Physical access controls for the facility.
4.2.9.4. Internal Security Awareness and Training curriculum and syllabus, new employee class schedule, annual refresher training, and any emergency, ad-hoc training.
4.2.9.5. Self-audit on all software and hardware, modifications, patches applied, etc. This report must be submitted at least twice per annum.
4.2.9.6. Backup, restore, and disaster recovery procedures and any associated test results. This includes results from the annual Disaster Recovery exercise.
4.2.9.7. Security Incident Response and Reporting Policies and Procedures.
4.2.9.8. Production Change Management Policies and Procedures.
4.2.9.9. Event Logging & Auditing Policies and Procedures for Networks, Operating Systems, Applications, and Databases.
4.2.9.10. Any third-party Risk and/or Audit and/or Vulnerability Assessment report.
4.2.9.11. Absent an ability to meet the annual assurance requirements specified in System and Services Acquisition Policy and Procedures (SA-1),[12] provide any up-to-date Compliance Report. (Also see the previous provision.)
4.2.9.12. Based on the sum-total of the above submissions and the data being handled, the CISO *may* allow a CSP some easement of the reporting requirements in this section, and/or an interim authority to operate

[12] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemAndServicesAcquisitionPolicy.pdf

until the requisite requirements can be met. However, in and of itself, a third-party Risk and/or Audit and/or Vulnerability Assessment report does *not* entitle a blanket exemption from any I.T. policy.

4.3. Agency Contract Administrator:
- 4.3.1. Enforces this Policy.
- 4.3.2. Consults with the Attorney General's Office, as necessary, in the enforcement of this Policy.
- 4.3.3. Collaborates with DAFS I.T. Procurement, the CISO, and the OIT Service Directors and Account Managers, in the enforcement of this Policy.
- 4.3.4. Ensures applicable Requests for Proposals (RFPs), and resulting Contracts, contain language that is in accordance with this Policy.
- 4.3.5. Ensures applicable State of Maine procurement instruments (RFPs, Contracts etc.), specify all required compliance standards, and all Federal and Maine Laws, Regulations, Statutes, and Rules, relevant to Remote (Cloud) hosting, including, but not limited to, those listed in Item 4.2.2 above.
- 4.3.6. Ensures that applicable Contracts contain language that explicitly state:
  - 4.3.6.1. All accounting, records, and audit compliance requirements, commensurate with the classification of data being transacted, and its specific oversight stipulations.
  - 4.3.6.2. All data ownership directives.
  - 4.3.6.3. All data residency directives.
  - 4.3.6.4. All data handling and transfer directives.
  - 4.3.6.5. All Cyber Liability directives, pegged to the number of unique PII records.
  - 4.3.6.6. Scheduled Uptime requirements. Unless otherwise specified in the Contract, by default, 99.9% scheduled uptime, excluding planned downtime for maintenance, is required.
  - 4.3.6.7. Performance/response time requirements, for both data inquiry/lookup and data modification transactions.
  - 4.3.6.8. RTOs and RPOs.

4.4. OIT Information Asset Owners and Account Managers:
- 4.4.1. Assist the Agency Contract Administrator in the enforcement of this Policy.
- 4.4.2. Ensure that the hosted information asset complies with the Application Deployment Certification Policy[13] prior to their deployment.
- 4.4.3. Maintain the status of the hosted information asset in the OIT Asset Inventory.
- 4.4.4. Evaluate the business impact of a security incident notification from the CSP, and liaise with the affected business stakeholders.
- 4.4.5. Evaluate the business impacts of the Uptime and Unplanned Outage Report and Planned Downtime Notice Report from the CSP, and liaises with affected business stakeholders.

[13] https://www.maine.gov/oit/policies/Application-Deployment-Certification.pdf

4.5. DAFS I.T. Procurement:
4.5.1. Assists the Agency Contract Administrator in the enforcement of this Policy.

5.0. Directives

5.1. Complete and exclusive ownership of the State of Maine information asset (including data, metadata, and log) rests with the State of Maine, and is not subject to any conditions.

5.2. Data residency always remains within the Continental United States.

5.3. Any State of Maine information asset (including data, metadata, and log) must be isolated/segregated/containerized such that no other fellow-consumer of the Remote hosting (Cloud) service may ever gain access to the State of Maine information asset under any circumstance. To fully achieve this requires implementing security controls in multiple layers (application, platform, and infrastructure), and in areas including, but not limited to, architecture, identity and access management, isolation, and data protection. State of Maine information assets (data, metadata, and log) must *never* reside in a shared, multi-tenant data repository without multi-layered, multi-pronged isolation/segregation/containerization.

5.4. The exact distribution of technical responsibilities, and the Information Assurance burden, between the State and the CSP, depends upon the layer at which the Remote (Cloud) service is consumed.
5.4.1. For SaaS, the CSP delivers the entire technology stack, and bears the entire Information Assurance burden. Both the State and the CSP must collaborate toward any Virtual Private Network connectivity, and interfaces.
5.4.2. For PaaS, the CSP delivers the platform, whereas the State (potentially in collaboration with other partners) creates the end-user application. The CSP's Information Assurance burden is limited to the platform. Both the State and the CSP must collaborate toward any Virtual Private Network connectivity, and interfaces.
5.4.3. For IaaS, the CSP delivers the hypervisor,[14] whereas the State (potentially in collaboration with other partners) creates everything above it, up to, and including, the end-user application. The CSPs Information Assurance burden is limited to the hypervisor. The State acquires and owns the tenant/container/org/presence within the IaaS CSP. Further, it is the State's responsibility (potentially in collaboration with other partners) to maintain any necessary isolation amongst the information assets within that tenant/container/org/presence. Both the State and the CSP must collaborate toward any Virtual Private Network connectivity, and interfaces.

[14] https://en.wikipedia.org/wiki/Hypervisor

5.5. Upon termination of the contract, the CSP must:
- 5.5.1. Return/transfer all Confidential Information, stored in any format, and, following the return/transfer, destroy any residual Confidential Information in the possession of the CSP.
- 5.5.2. Submit to OIT on the CSP's letterhead a "CERTIFICATION OF RETURN/TRANSFER AND DESTRUCTION OF CONFIDENTIAL INFORMATION, ELECTRONIC INFORMATION, AND TANGIBLE PROPERTY" certifying that all copies of Confidential Information, electronic property, and tangible property belonging to the State or OIT have been returned/transferred, and, any residual components of the same have been destroyed.
- 5.5.3. The target of the return and/or transfer of the State of Maine information assets (including data, metadata, and log) may involve another Agent of the State of Maine (potentially, another CSP), within a timeline and method agreed to by the Agency Contract Administrator.
- 5.5.4. Comply with audit verification to ensure that all State of Maine information assets (including data, metadata, and log) have indeed been returned/transferred.
- 5.5.5. Destruction of any residual State of Maine information asset footprint, including archival/backup copies, must comply with the NIST 800-88[15]

5.6. The CSP bears the full remediation costs of any security vulnerability, and/or breach, that unambiguously results from verifiable CSP negligence. In addition to this Policy, current NIST policies, and industry best practices will be used to determine what constitutes CSP negligence. The CISO and the Agency Contract Administrator jointly decide on this matter.

6.0. Document Details

6.1. Initial Issue Date: 8 January 2007
6.2. Latest Revision Date: 20 October 2023
6.3. Point of Contact: Enterprise.Architect@Maine.Gov
6.4. Approved By: Chief Information Officer, OIT
6.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[16]
6.6. Waiver Process: Waiver Policy[17]
6.7. Distribution: Internet[18]

[15] https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
[16] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[17] https://www.maine.gov/oit/policies/waiver.pdf
[18] https://www.maine.gov/oit/policies