



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

## Information Security Policy

### 1.0 Statement

The Information Security Policy establishes the *minimum* benchmark to protect the security of State *Information Assets*<sup>1</sup> through a layered structure of overlapping controls and continuous monitoring.

### 2.0 Purpose

State information is a valuable asset that must be secure, both at rest and in transit, and protected from unauthorized use, disclosure, modification, and destruction. Appropriate controls and procedures must be instituted to ensure that its confidentiality, integrity, and availability are not compromised.

### 3.0 Applicability

This Policy applies to all Information Assets under the purview of the Chief Information Officer (CIO), irrespective of where the Information Assets are hosted.

### 4.0 Responsibilities

- 4.1 The Associate CIO, Infrastructure executes this Policy for all Information Assets.
- 4.2 The Enterprise Security Officer (ESO) owns, interprets, and enforces this Policy.
- 4.3 The *Agency Data Custodian*<sup>2</sup> executes this Policy for all Information Assets under their purview.

### 5.0 Directives

- 5.1 **Access Authorization:** Access to any State Information Asset must be authorized by the Agency Data Custodian.
- 5.2 **Access Control:** Access to any State Information Assets must be based upon each user's access privileges. This access may be restricted by day, date, and time, as appropriate.

---

<sup>1</sup> Information Assets: Business applications, system software, development tools, utilities, hardware, infrastructure, paper records, etc.

<sup>2</sup> Agency Data Custodian: Agency official, who, based on their position, is fiduciary owner of specific Agency Information Assets. For instance, the Labor Bureau of Unemployment Compensation Director (or designee) is the Agency Data Custodian for Unemployment Compensation Information Assets, and the Health & Human Services Office of Family Independence Director (or designee) is the Agency Data Custodian for Benefits Information Assets.

Access privileges shall be granted based on *Least Privilege Access*<sup>3</sup>.

**5.3 Access – Non-State Entities:** OIT is responsible for analyzing the security risks whenever non-State entities access State information, and ensuring that such access is in full compliance with ALL relevant OIT policies, practices, and procedures.

- 5.3.1 Any contract with a non-State entity involving access to State Information Assets must include an explicit provision binding the non-State entity to full compliance with ALL relevant OIT policies, practices, and procedures.
- 5.3.2 Non-State access privilege must be based on Least Privilege Access, commencing as late as practically possible and terminating as soon as the underlying business requirement ceases to exist.
- 5.3.3 The burden of justification rests entirely on the Agency Data Custodian, who is responsible for applying to the ESO for said access. Access is contingent upon explicit approval from the ESO, and is subject to revocation by the ESO at any time. It remains the burden of the Agency Data Custodian to apprise the ESO re: any change in business requirement and/or the status of the non-State entity.

**5.4 Access Rights Review:** Periodic log reviews of user access and privileges must be performed by the Agency Data Custodian in order to monitor access to State Information Assets, as well as deviations from authorized usage.

**5.5 Background Checks:** OIT will comply with any Federal/State background check requirements for its employees and contractors.

**5.6 Backups:** Backups of all State Information Assets must be routinely created and properly stored to ensure prompt restoration, when necessary. Backups must be handled with exactly identical care and precaution as the original Information Asset itself. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must meet customer expectations on a per Information Asset basis.

**5.7 Data Classification:** Agency Data Custodians must collaborate with the Enterprise Security Officer in adopting and adhering to an information classification system, the purpose of which is to ensure that all Information Assets are operated in a manner compliant with any and all applicable State and Federal regulations.

- 5.7.1 *High Risk:* Information Assets for which there exist legal regulations and/or penalties for disclosure. Data covered by Federal and State legislation, such as CJIS, FERPA, HIPAA, IRS 1075, or the Data Protection Act, are in this class. In general, criminal justice, health, payroll, personnel, and financial data belong in this class. Other data included in this class include information that, if compromised, would cause severe damage to the State. The Agency Data Custodian makes this determination.
- 5.7.2 *Restricted:* Data that may not cause severe damage to the State if it were to be compromised, but the Agency Data Custodian still desires to protect against unauthorized disclosure and/or modification. Again, the Agency Data Custodian makes this determination.
- 5.7.3 *Public:* Information that may be freely disseminated.

---

<sup>3</sup> Least Privilege Access: A security principle where users are assigned access that is just adequate enough to perform their job responsibilities. Access is granted for the shortest duration possible.

5.7.3.1 Agency Data Custodians must determine the data classification and must ensure that data is protected in a manner commensurate with its classification.

5.7.3.2 No Information Asset must be exposed to the Internet without the means to protect it in a manner commensurate with its classification.

5.8 **Discipline:** State and Agency-specific discipline will be executed against users who violate this Policy.

5.9 **Documentation:** All Information Assets must include sufficient documentation to satisfy any applicable audit and security policy requirements.

5.10 **Education & Training:** Information security training must be conducted and documented annually for all Agency personnel in accordance with [Executive Order 2014-003<sup>4</sup>](#). Such training must include security awareness, updates to security policies or procedures, and reporting of incidents, and vulnerabilities. Agency Data Custodians will ensure that their Agency employees and contractors comply with any other applicable Federal/State requirements for security awareness, education, and training.

5.10.1 OIT will partner with State Agencies to deliver Security Awareness Training contents customized for individual Agencies.

5.10.2 All personnel within an Agency with access to State Information Assets must complete the targeted Security Awareness Training, once per annum, within a span of eight weeks.

5.11 **Incident Reporting:** Any OIT employee or contractor that becomes aware of a *potential* security incident should immediately notify their management. Non-OIT State employees or contractors who suspect an information security incident should immediately notify OIT Customer Support (624-7700) and follow any applicable Agency-specific procedures.

5.12 **Information Asset Maintenance:**

5.12.1 All products must be fully supported by the original product vendor (or an accountable other-party). This includes "Extended Support", not just "Service Pack" or "Mainstream Support".

5.12.2 Any and all systems hosting State information must be current with all security patches.

5.12.3 All connections to the Internet must go through a properly secured access point provided by OIT to ensure that the State network is protected.

5.13 **Interconnection Security Agreements:** Specific agreements enforcing appropriate information security controls must be instituted for any information exchange among Agencies, as well as other external entities. At a minimum, the sender of the information must impose upon the receiver the very same stipulations that the sender is subject to vis-à-vis the information.

5.14 **Malwares:**

---

<sup>4</sup> <http://www.maine.gov/tools/whatsnew/attach.php?id=626944&an=1>

- 5.14.1 Awareness, prevention, detection, and neutralization controls must be utilized to protect State Information Assets against malwares (rogue applications that disrupt the normal functioning of computers).
- 5.14.2 Willful introduction of malwares into the State network is prohibited.
- 5.14.3 Any and all devices that connect to the State network must be protected with an approved, licensed anti-malware that it is kept updated according to the anti-malware vendor's recommendations.
- 5.14.4 All State infrastructure Information Assets must be hardened, and logs monitored, to protect against malwares.

**5.15 Passwords:** Access to any State Information Asset must be through individual and unique logins, and must require authentication. By default, shared accounts must not be used. Authentication includes the use of passwords, smart cards, biometrics, challenge-response questionnaire, or such other industry-accepted best practices. Any device used for authentication (SecurID token, etc.) is to be used by the assigned individual only, and must not be shared. Users must select, employ, and manage passwords to protect against unauthorized discovery or usage. All users of high risk or restricted data must have a strong password, the definition of which will be established and documented by OIT, taking into account such features as length, complexity, unpredictability, expiration frequency, etc. Credentials for empowered accounts (such as administrator, root, or supervisor) must be changed frequently, consistent with guidelines established by OIT. Credentials for empowered accounts must be modified any time the underlying system is installed, rebuilt, or reconfigured. Service accounts that do not allow login are not considered empowered accounts. All default passwords must be modified immediately post-installation. Passwords must never be stored or transmitted without first having been hashed or encrypted.

**5.16 Physical Protection:** Where applicable, State infrastructure Information Assets must be protected from physical and environmental threats in access controlled environments.

- 5.16.1 Both OIT and Agencies must institute appropriate measures to prevent and detect unauthorized access or damage to facilities that contain State Information Assets. Facilities that house State infrastructure Information Assets must utilize physical access controls designed to permit access by *Authorized Users*<sup>5</sup> only.

**5.17 Remote, Mobile, and Wireless Access (Safeguarding Portable and Mobile Devices):** Agencies must comply with the Remote Access methods provided by OIT when remotely accessing the State network. Agencies must comply with the Wireless Access methods provided by OIT when wirelessly accessing the State network.

- 5.17.1 When Agencies approve teleworking for their personnel, they must ensure that the security of State Information Assets is not compromised.
- 5.17.2 Agency Data Custodians will safeguard High Risk and Restricted information stored on portable devices (laptops, pocket personal computers, hand-held devices, USB thumb drives, smart phones, etc.) by:

- 5.17.2.1 Properly classifying any data stored on personal devices

---

<sup>5</sup> Authorized User: An individual who has approved access to an Information Asset in order to perform job responsibilities.

- 5.17.2.2 Using encryption to safeguard data and prevent unauthorized access
- 5.17.2.3 Requiring written authority to copy data to portable devices
- 5.17.2.4 Ensuring that all Agency personnel (employees and contractors) who use portable devices are aware of, and comply with this policy and any other applicable Federal or State legislation regarding data on portable devices.

**5.18 Risk Assessments:** State Information Assets will be assessed for security risks and priority risks will be promptly addressed. The Enterprise Security Officer will:

- 5.18.1 Ensure that applicable security tests as defined in the [Application Deployment Certification Policy](#)<sup>6</sup> are performed.
- 5.18.2 Ensure that applicable security tests as defined in the [Infrastructure Deployment Certification Policy](#)<sup>7</sup> (if OIT-Hosted), or as defined in the [Remote Hosting Policy](#)<sup>8</sup> (if Remote-Hosted) are performed.
- 5.18.3 Authorize random and scheduled information security risk assessments to evaluate State computer devices, operating systems, and applications, including websites, for risk vulnerabilities pertaining to confidentiality, integrity, and availability.
- 5.18.4 Coordinate security risk assessments with the Technology Business Consultant (TBC) of the agency who owns the system in order to minimize disruptions to operations. When the ESO identifies a potential high-risk situation, these assessments may be conducted without advance scheduling.
- 5.18.5 Alert the TBC and applicable OIT Leadership whenever a critical information security deficiency is discovered. The TBC serves as the communication liaison to key Agency personnel.
- 5.18.6 In the event of a significant security risk, at their discretion, remove the computer device or application from service until the risk is mitigated or until an approved waiver is in place.
- 5.18.7 Prepare and provide a report of the security risk findings to key OIT personnel, including the TBC. The TBC will handle any dissemination to the agency.

**5.19 Rules of Behavior<sup>9</sup> for All Users:** All users must comply with the following standards:

- 5.19.1 Must not attempt to access any Information Asset for which they do not have express authorization.
- 5.19.2 Must not divulge remote connection methods and protocols.
- 5.19.3 Must not share their credentials.
- 5.19.4 Must not use non-standard software or equipment.
- 5.19.5 Must exercise caution when accessing emails, attachments, hypertext links, etc. from unknown sources.
- 5.19.6 Must not make unauthorized changes.
- 5.19.7 Must not insert any removable media into a State device without ensuring that it does not contain malware.
- 5.19.8 Must not allow others to use their account or access other users' accounts.

---

<sup>6</sup> <http://www.maine.gov/oit/policies/Application-Deployment-Certification.htm>

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

<sup>8</sup> <http://www.maine.gov/oit/policies/RemoteHostingPolicy.htm>

<sup>9</sup> Rules of Behavior: Behavioral standards to facilitate information security, especially relevant to Privileged Users.

- 5.19.9 Must comply with agency-specific procedures and protocols while transferring files. They must also report any security weakness to the appropriate agency personnel. Security weakness includes unexpected system behavior, which may result in unintentional disclosure of information or exposure to security threats.
  - 5.19.10 Must not engage in activity that may degrade the performance of Information Assets, deprive an Authorized User access to resources, obtain extra resources beyond those allocated, or circumvent other security measures.
  - 5.19.11 Must not download, install, or execute utilities such as password crackers, packet sniffers, or port scanners that reveal or exploit security weaknesses.
  - 5.19.12 Must sign and comply with agency-specific non-disclosure and confidentiality agreements
  - 5.19.13 Must adhere to additional requirements stipulated by OIT regarding personal devices.
  - 5.19.14 Must not download/transfer sensitive information to any non-State device.
  - 5.19.15 Must comply with supplemental rules, beyond the ones listed above, for specific systems, as needed.
  - 5.19.16 System utilities will be made available only to those who have a legitimate business case for a specific utility.
- 5.20 **Rules of Behavior for *Privileged Users***<sup>10</sup>: Due to privileged access rights, these users must also comply with standards higher than ordinary users. Applies only to server-class devices.
- 5.20.1 System Administration account (i.e. 'root') access must be limited to as small a group as possible and based on Least Privilege Access. For example, the 'root' account should not be used for tasks that can be completed via a non-privileged account.
  - 5.20.2 Any administrators must first login as themselves (ordinary user) before escalating privileges to that of an administrator.
- 5.21 **Session Timeout**: The session activity timeout is 15 minutes. Any session that is inactive for more than 15 minutes must either log off the user or lock the session until fresh re-authentication.
- 5.22 **Static Storage (Data at Rest)**: Static storage of state information outside the state firewall that contains Personally Identifiable Information<sup>11</sup> (or other High-Risk data) must be encrypted to at least the current NIST-approved standard for encryption of static data.
- 5.23 **Storage Media Disposal**: When no longer required, ALL storage media (both fixed and removable) must be permanently scrubbed or destroyed or rendered unrecoverable in accordance with applicable State, Federal, or Agency regulations.
- 5.23.1 Media may be scrubbed by being degaussed.
  - 5.23.2 Alternatively, media maybe sanitized in accordance to [NIST Special Publication 800-88](#)<sup>12</sup>. A simple wiping method maybe implemented in the following way: Pass 1:

---

<sup>10</sup> Privileged User: The user granted the rights that go beyond that of a typical business user to manage and maintain IT systems. Usually, such rights include administrative access to networks and/or devices. This does not include users with administrative access to their own workstation.

<sup>11</sup> Personally Identifiable Information: information that can be used to identify a single person, such as name, social security number, date and place of birth, mother's maiden name, driver's license, biometrics, etc. Maine State law also has a more specific definition in [10 M.R.S. §1347](#)

<sup>12</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

Writes a zero and verifies the write; Pass 2: Writes a one and verifies the write; Pass 3: Writes a random character and verifies the write.

5.23.3 Physical destruction of media should be conducted by a qualified vendor.

**5.24 Transport Security (Data in Flight):** Any transmission (including E-Mail, file transfer, etc.) of Personally Identifiable Information (or other High-Risk data) must be encrypted to at least the current standard for Transport Layer Security (such as NIST or FIPS or per the specific Agency's State/Federal requirements).

5.24.1 Any application that has end-users (portal-type application, etc.) requires a commercial-grade certificate. It is acceptable to use self-signed certificates for applications without end-users (device to device connectivity) as long as they have trusted endpoints.

5.24.2 Authentication must be conducted under an encrypted tunnel to at least the current NIST-approved standard for Transport Layer Security.

**5.25 Unknown Custody Device:**

5.25.1 All personnel must maintain safe custody of any and all State devices, including removable media (such as memory sticks).

5.25.2 When device custody cannot be verified, including a found device, it must be sent to Enterprise Security Officer (State House Station #145) for verification.

5.25.3 If, and only if, the Enterprise Security Officer green-lights the subsequent use of that found device should it be put back into State use.

**5.26 Vulnerability Management:** Vulnerabilities in networks, devices, and applications present a risk to State Information Assets. Vulnerability Management is the formal procedure of identifying, classifying, remediating and/or mitigating vulnerabilities. The ESO is responsible for classifying vulnerabilities. They are classified as follows:

5.26.1.1 *High (Critical):* Allows a remote attacker to gain administrative control.

5.26.1.2 *Medium (Severe):* Allows a remote attacker to gain user-level control, or to cause shutdown/reboot/instability.

5.26.1.3 *Low:* Unlikely to directly compromise security but might still provide a remote attacker with a springboard for privilege-escalation.

5.26.2 When a patch or known workaround is discovered, by default vulnerabilities must be handled accordingly:

5.26.2.1 High (Critical) - Within 30 days

5.26.2.2 Medium (Severe) - Within 60 days

5.26.3 While no specific timeline is listed for *Low* vulnerabilities, these should not be ignored. The ESO will determine whether any vulnerability (*High, Medium, or Low*) represents an escalated risk and requires more immediate attention.

5.26.4 Typically, vulnerabilities are addressed by applying vendor supplied patches. However, compensating controls can alternatively be used to address identified vulnerabilities given potential flaws in patches, potential difficulties removing flawed patches from systems, and potential scheduling issues patching production systems.

- 5.26.5 If utilized, compensating controls must provide the same or greater level of defense as would be attained through patching. Compensating controls can be used as an interim solution (until the next maintenance/patching schedule) or as a longer-term solution.

## **6.0 Document Information**

This revision replaces the *Policy to Safeguard Information on Portable Computing and Storage Devices*, the *Standard to Safeguard Information on Portable Computing and Storage Devices*, the *Security Awareness Training Policy* and the *Policy to Govern Information Security Risk Assessments of State Computer Systems and To Ensure the Prompt Remediation of Deficiencies*.

Initial Issue Date: May 1, 2012

Latest Revision Date: January 23, 2017 – to update Document Information.

Point of Contact: Architecture-Policy Administrator, OIT, [Enterprise.Architect@Maine.Gov](mailto:Enterprise.Architect@Maine.Gov)

Approved By: Chief Information Officer, OIT

Legal Citation: [Title 5, Chapter 163: Office of Information Technology](#)<sup>13</sup>.

Waiver Process: See the [Waiver Policy](#)<sup>14</sup>.

---

<sup>13</sup> <http://legislature.maine.gov/statutes/5/title5ch163sec0.html>

<sup>14</sup> <http://www.maine.gov/oit/policies/waiver.htm>