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

System and Information Integrity Policy and Procedures (SI-1)

Table of Contents

1.0 Document Purpose

The purpose of this document is to define the State of Maine policy and procedures that are in place to ensure system and information integrity for State of Maine information assets (see Definitions). This part of the security program is focused on protecting the confidentiality (see Definitions), integrity (see Definitions), and availability (see Definitions) of State information assets. This document corresponds to the System and Information Integrity Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0 Scope

2.1 This policy applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

- 2.1.1 Executive Branch Agency information assets, irrespective of location; and
- 2.1.2 Information assets from other State government branches that use Executive Branch managed services.

3.0 Policy Conflict

If this policy conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0 Roles and Responsibilities

4.1 Agencies

- 4.1.1 Manage agency data in a secure manner.
- 4.1.2 Ensure that any contracts for vendor-hosted or -managed agency information systems adhere to any pertinent Federal regulations, State regulations, and Office of Information Technology (OIT) policies, procedures, and standards.
- 4.1.3 Ensure agency personnel are aware of penalties for noncompliance.
- 4.1.4 Develop and implement agency-level policy and procedures to meet additional pertinent system and information integrity statutory requirements.

4.2 OIT

- 4.2.1 Assigns an owner for each infrastructure information asset (for example, network, firewall) it supports (see the appendix).

4.3 OIT Information Asset Owners

- 4.3.1 Ensure that systems and information integrity protections are in place for their assigned information asset(s).
- 4.3.2 Implement security directives.
- 4.3.3 Protect information system memory from unauthorized code execution.
- 4.3.4 Utilize standard operating procedures to manage required changes.
- 4.3.5 Utilize integrity verification tools to detect unauthorized changes to software and information.

4.3.6 In collaboration with IT Procurement and agencies, hold contracted other parties that host State information assets accountable to this Policy and Procedures.

4.4 Information Security Office
- 4.4.1 Identifies and reports information system flaws.
- 4.4.2 Performs scheduled information system security scans.
- 4.4.3 Protects information systems from malicious code.
- 4.4.4 Monitors information systems.

4.5 IT Procurement
- 4.5.1 In collaboration with Information Asset Owners and agencies, hold contracted other parties that that host State information assets accountable to this Policy and Procedures.

5.0 Management Commitment

The State of Maine is committed to following this policy and the procedures that support it.

6.0 Coordination Among Agency Entities

OIT provides system information and integrity at the enterprise level for infrastructure consumed by agency information systems. Agencies coordinate with OIT account managers, application development managers, and client technologies support staff to address agency-specific system and information integrity requirements. Application development managers serve as information asset owners for the agency information systems that their teams support.

7.0 Compliance

7.1 For State of Maine employees, failure to comply with the procedures identified in this policy may result in progressive discipline up to and including dismissal.

7.2 For State of Maine contractors and non-State of Maine personnel, failure to comply may result in removal of the individual's ability to access and use State of Maine data and systems. Employers of non-State of Maine personnel will be notified of violations.

7.3 Personnel are also subject to penalties for violations of statutory compliance requirements. Depending on the requirement and the nature of the violation, penalties can include fines and criminal charges.

8.0 Procedures

The following standards apply to, and represent, the security controls established to meet an acceptable level of protection for, State of Maine information systems. They serve as the base set of procedural requirements that are implemented to provide system and information integrity.

8.1 Flaw Remediation (SI-2, SI-2(1), SI-2(2))

8.1.1 Agencies, in consultation with OIT, ensure that appropriate mechanisms are in place to identify, report, and correct flaws in agency information systems.

8.1.2 The Information Security Office employs the following mechanisms, in accordance with the above:

- 8.1.2.1 Subscribes to Multi-State Information Sharing and Analysis Center (MS-ISAC) alerts and MITRE Common Vulnerabilities and Exposures (CVE) updates and notifications.
- 8.1.2.2 Distributes alerts, updates, and notifications to information asset owners.
- 8.1.2.3 Scans information systems weekly and monthly at set intervals.
- 8.1.2.4 Reviews all security-related reports.

8.1.3 OIT information asset owners take the following actions to correct information system flaws:

- 8.1.3.1 Conduct security testing in accordance with deployment certification procedures (see the Application Deployment Certification Policy[1] and the Infrasturure Deployment Policy[2]).
- 8.1.3.2 Install operating system patches and hot fixes (see Definitions).
- 8.1.3.3 Install security patches.
- 8.1.3.4 In collaboration with agencies and IT Procurement, utilize support and maintenance contracts to engage vendors in correcting identified flaws in off-the-shelf software or firmware.

8.1.4 OIT information asset owners utilize standard operating procedures to manage change. They:

- 8.1.4.1 Use the centrally managed OIT Change Advisory Board for change management.
  - 8.1.4.1.1 Production changes must follow the OIT Change Management Policy[3].
- 8.1.4.2 Install security-relevant software and firmware at defined intervals:
  - 8.1.4.2.1 The Information Security Office ensures that antivirus definition files are updated daily.
  - 8.1.4.2.2 Information asset owners install patches at predefined intervals for the information assets they manage (such as security patches for hosting environments).
  - 8.1.4.2.3 Information asset owners install patches, hot fixes, and service packs, as necessary, to address specific issues, such as identified critical vulnerabilities, that cannot wait for the next scheduled cycle.

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ApplicationDeploymentCertification.pdf
[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/Infrastructure-Deployment-Certification.pdf
[3] https://www.maine.gov/oit/policies/ChangeManagementPolicy.pdf

8.1.4.2.3.1 This determination is made in collaboration with the Information Security Office.

8.1.4.2.3.2 Alternatively, interim compensating controls, approved by the Information Security Office, may be used to address identified vulnerabilities.

8.1.5 The Information Security Office employs automated mechanisms (monthly scans), independent of patching schedule, to determine the flaw remediation status of information system components.

8.2 Malicious Code Protection (SI-3, SI-3(1), SI-3(2))

8.2.1 Agencies, in consultation with OIT, ensure that malicious code (see Definitions) protections are in place to detect and eradicate malicious code at agency information system entry and exit points.

8.2.2 OIT information asset owners implement malicious code protections at entry and exit points for the information asset they are responsible for. For example, Network Services utilizes firewalls to perform real-time scans at network entry and exit points to detect and eradicate malicious code.

8.2.3 OIT information asset owners keep malicious code protection mechanisms current by implementing new product releases when they become available. OIT information asset owners determine whether to update malicious code protections automatically or manually.

8.2.4 The Information Security Office employs products at information system entry and exit points to detect and eradicate malicious code.

8.2.4.1 The Information Security Office ensures antivirus definition files are updated daily. In addition, the Information Security Office configures products to perform weekly scans of information systems and to perform real-time scans of files from external sources.

8.2.4.2 The Information Security Office configures products to block and quarantine malicious code, and to alert the Information Security Office, in response to malicious code detection.

8.2.4.3 The Information Security Office reviews quarantined code for potential information system impact, and, if appropriate, sends it to the vendor for further analysis.

8.2.4.4 Quarantines are adjusted, based on the risk level of the finding (for example, considering false positives identified during analysis).

8.2.5 OIT manages malicious code protection centrally, at the enterprise level, as follows:

8.2.5.1 The Information Security Office and OIT information asset owners plan, implement, assess, authorize, and monitor malicious code protection products.

8.2.5.2 The Information Security Office consumes the MS-ISAC as a resource to plan, implement, assess, authorize, and monitor Albert.[4]

8.3 Information System Monitoring (SI-4, SI-4(1), SI-4(2), SI-4(4), SI-4(5), SI-4(7), SI-4(14))

8.3.1 Agencies, in consultation with OIT, ensure their agency information systems are monitored to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections.

8.3.2 In accordance with the above, OIT performs the following information system monitoring:

8.3.2.1 The Information Security Office employs products to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections.

8.3.2.2 The Information Security Office receives notifications for improper logins, as well as unexpected behaviors, to identify unauthorized use of information systems.

8.3.2.3 The Information Security Office deploys products strategically within information systems to collect essential information and at ad hoc locations within information systems to track specific types of transactions (such as hypertext transfer protocol (HTTP) traffic that bypasses HTTP proxies).

8.3.2.4 OIT information asset owners perform information system monitoring for the information asset they are responsible for. For example, Network Services employs firewalls to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections.

8.3.2.5 The Information Security Office and information asset owners protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion by requiring team administrator credentials.

8.3.2.5.1 Access to this information must be granted based on the principle of least privilege (see Definitions).

8.3.3 The Information Security Office heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations assets, individuals, other organizations, or the Nation, based on law enforcement information, intelligence information, or other credible sources of information. Heightened activity may include any of the following actions, based on the Information Security Office assessment of the situation:

[4] https://www.cisecurity.org/services/albert-network-monitoring/

8.3.3.1 The Information Security Office increases the involvement of external security analysts.

8.3.3.2 The Information Security Office and information asset owners leverage additional external incident response resources.

8.3.3.3 The Information Security Office consults with the Attorney General's Office and security legal analysts to obtain legal opinion regarding information system monitoring activities in accordance with applicable Federal or State laws, executive orders, directives, policies, or regulations.

8.3.4 The Information Security Office employs products to provide intrusion detection.

8.3.5 Network Services employs intrusion detection and intrusion prevention systems on network entry to detect attempted intrusions into the enterprise.

8.3.5.1 Logs are automatically imported into a central security information and event management (SIEM) repository for anomaly alerting and processing.

8.3.6 Network Services employs firewall intrusion detection and intrusion prevention systems.

8.3.7 Network Services employs products to monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.

8.3.8 Network Services employs access points and wireless local area network controllers for over-the-air detection and reporting.

8.3.9 The Information Security Office and OIT information asset owners employ systems that alert teams when indications of compromise or potential compromise occur.

8.3.9.1 Automated mechanisms are employed, where available, to alert security personnel of unusual or inappropriate activities that have security implications. Manual mechanisms are used in instances where automatic mechanisms are not implemented.

8.3.9.2 When suspicious events are detected, designated agency personnel are notified, and necessary actions are taken to address the suspicious events.

8.4 Security Alerts, Advisories, and Directives (SI-5)

8.4.1 Agencies, in consultation with OIT, ensure that mechanisms are in place to receive security alerts, advisories, and directives on an ongoing basis, that are pertinent to their agency information systems.

8.4.2 The Information Security Office team receives and disseminates system security alerts, advisories, and directives on an ongoing basis from multiple sources, including:
- 8.4.2.1 MS-ISAC emails;
- 8.4.2.2 Albert suspicious internet traffic report; and
- 8.4.2.3 The Department of Homeland Security.

8.4.3 The Information Security Office generates internal security alerts, advisories, and directives as deemed necessary (for example, in response to a known issue or threat or to strengthen the State's security posture).
- 8.4.3.1 The audience for the communication is determined based on the nature of the alert, advisory, or directive (technical, agency end user, agency leadership).
- 8.4.3.2 Agency communication is coordinated through the OIT account managers, communications manager, or application development managers.
- 8.4.3.3 OIT technical communication is handled directly by the Information Security Office.
- 8.4.3.4 The Information Security Office establishes security directive implementation time frames and notifies OIT information asset owners as part of the communication.

8.5 Security Function Verification (SI-6)

8.5.1 Agencies, in consultation with OIT, ensure that mechanisms are in place to verify the correct operations of organizationally defined security functions (see Definitions) that are pertinent to their agency information systems.

8.5.2 The Information Security Office identifies defined security functions at an enterprise level.

8.5.3 Agencies must identify any supplemental security functions necessary to meet regulatory requirements.

8.5.4 Agencies collaborate with their application development managers and/or account managers to implement supplemental security functions for OIT-supported agency information systems.

8.5.5 The Information Security Office works with information asset owners (typically system administrators) to review and verify configuration settings and deployment certifications to ensure security functions are implemented.

8.5.6 On a scheduled basis (at a frequency determined by the information asset owner in collaboration with the Information Security Office), information asset owners conduct patching and verification.

8.5.7 If there is a failed security test, the Information Security Office notifies and works with information asset owners to address identified issues.

8.5.8 The information asset owner takes necessary action to address any identified issues (e.g., shut down or restart the information asset, etc.).

8.6 Software, Firmware, and Information Integrity (SI-7, SI-7(7))

8.6.1 Agencies, in consultation with OIT, ensure that integrity verification tools are employed to detect unauthorized changes to software and information.

8.6.2 OIT information asset owners utilize integrity verification tools to detect unauthorized changes to software and information (such as network and security infrastructure tools).

8.6.3 The Information Security Office conducts integrity scans of information systems on an as-needed basis to assess the integrity of software and information.

8.6.4 The Information Security Office classifies unauthorized security-relevant changes that are detected and reported and determines whether they are subject to formal incident-response procedures.

8.7 Spam Protection (SI-8, SI-8(1), SI-8(2))

8.7.1 Agencies, in consultation with OIT, ensure that spam (see Definitions) protection mechanisms are employed at agency information system entry and exit points to detect and act on unsolicited messages.

8.7.2 OIT information asset owners employ spam protections, in accordance with the above, for the information asset that they manage.

- 8.7.2.1 In Microsoft 365, email messages are automatically protected against spam and malware by Exchange Online Protection (EOP).
- 8.7.2.2 EOP has built-in inbound and outbound malware filtering to help protect the State of Maine from malicious software, and built-in spam filtering to help protect the State of Maine from both receiving and sending spam (for example, in case of compromised accounts).
- 8.7.2.3 Admins don't need to set up or maintain the filtering technologies because they're enabled by default.
- 8.7.2.4 For SharePoint Online, anti-malware protection is automatically provided for files that are uploaded and saved to document libraries. This protection is provided by the Microsoft anti-malware engine also integrated into Exchange. This anti-malware service runs on all SharePoint Online Content Front Ends.

8.8 Information Input Validation (SI-10)

8.8.1 This section applies to any information asset where OIT has ownership of the code.

8.8.2 Agencies, in consultation with OIT, ensure that their agency information systems check the validity of defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

8.8.2.1 Agencies define the information inputs subject to this validation and the method through which validation takes place, in consultation with OIT.

8.8.2.2 OIT application development managers ensure their teams implement input validation mechanisms for their assigned agency systems, in accordance with the above.

8.8.2.3 The Information Security Office validates the implementation through regular application vulnerability scanning.

8.9 Error Handling (SI-11)

8.9.1 Agencies, in consultation with OIT, ensure that their agency information systems generate error messages that provide information necessary for corrective action, without revealing information that could be exploited by adversaries. In addition, agencies must ensure that their information systems reveal error messages only to defined personnel and roles.

8.9.1.1 Agencies review error message content, prior to implementation, to ensure that no information is revealed that could be exploited by adversaries.

8.9.1.2 Agencies define the personnel and roles who error messages are revealed to.

8.9.1.3 OIT application development managers ensure that their teams implement error messages, in accordance with the above, for their assigned agency systems.

8.9.1.4 The Information Security Office team validates the implementation through regular application vulnerability scanning.

8.10 Information Handling and Retention (SI-12)

8.10.1 Agencies, in consultation with OIT, ensure that information asset output is handled and retained in accordance with data classification handling requirements, applicable State and Federal laws, directives, policies, regulations, standards, and operational requirements.

8.10.1.1 Agencies define information handling and retention standards in accordance with the above.

8.10.1.2 The OIT information asset owners implement agency-defined information handling and retention standards for the information asset they manage (for example, backup and recovery).

8.10.1.3 Archiving data according to specific business requirements is part of the application development process.

8.10.2 File Transfer Retention Period:

8.10.2.1 Files and folders transferred via file transfer systems will be retained for the least amount of time necessary to achieve the data

exchange but no longer than seven (7) days from the date of file or folder creation.

8.10.2.2 Historical records must not be stored on file transfer systems. Any long-term data retention need must be met and supported by other technology solutions.

8.11 **Memory Protection (SI-16)**

8.11.1 Agencies, in consultation with OIT, ensure that security safeguards are used to protect information system memory from unauthorized code execution.

8.11.2 For information assets where OIT has control of the code, the Information Security Office employs malicious code protection products to protect information system memory from unauthorized code execution.

9.0 Document Details

9.1 Initial Issue Date: July 19, 2019
9.2 Latest Revision Date: July 24, 2024
9.3 Point of Contact: Enterprise.Architect@Maine.Gov
9.4 Approved By: Chief Information Officer, OIT
9.5 Legal Citation: Title 5, Chapter 163: Office of Information Technology[5]
9.6 Waiver Process: Waiver Policy[6]
9.7 Distribution: Internet[7]

10.0 Review

This document is reviewed triennially and whenever substantive changes are made to policies, procedures, or other authoritative regulations that affect it.

11.0 Records Management

OIT security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures* and *Internal Control Policies and Directives* records management categories. They will be retained for 3 years and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to future State Archives General Schedule revisions that cover these categories.

12.0 Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA),[8] certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures, or risk assessments. Information contained in these records may be disclosed to the State Legislature or, in the case of a political or administrative subdivision, to municipal

[5] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[7] https://www.maine.gov/oit/policies-standards
[8] https://legislature.maine.gov/statutes/1/title1sec402.html

officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the State.

13.0 Definitions

13.1 Availability: Timely and reliable access to and use of information.[9]

13.2 Confidentiality: Preserving authorized restrictions on information acces and disclosure, including means for protecting personal privacy and proprietary information

13.3 Hot fix: A patch applied to a live system.

13.4 Information Asset: Used interchangeably with information system. A discrete, identifiable piece of information technology, including hardware, software, and firmware. Information assets include, for example, mainframes, workstations, servers (including database, electronic mail, authentication, web, proxy, file, and domain name), input/output devices (such as scanners, copiers, and printers), network components (such as firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, and sensors), operating systems, virtual machines, middleware, business applications, system software, development tools, and miscellaneous related utilities.

13.5 Integrity: The accuracy and consistency (validity) of data over its lifecycle. Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.

13.6 Malicious code: Unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Classifications of malicious code include viruses, worms, and Trojan horses.

13.7 Principle of Least Privilege: A security principle whereby users are assigned the minimum access necessary to perform their job responsibilities. Access is granted for the shortest duration possible.

13.8 Security function: The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

13.9 Spam: Unsolicited usually commercial messages (such as emails, text messages, or internet postings) sent to a large number of recipients or posted in a large number of places.

[9] https://csrc.nist.gov/glossary

14.0 Abbreviations

14.1 CVE: common vulnerabilities and exposures
14.2 EOP: Exchange Online Protection
14.3 HTTP: Hypertext Transfer Protocol
14.4 MS-ISAC: Multi-State Information Sharing and Analysis Center
14.5 OIT: Office of Information Technology
14.6 SIEM: security information event management

Appendix – Office of Information Technology Information Assets and Services

Information Asset/Service	Description	Owner
Business applications	OIT-developed applications to support specific business functions	Enterprise Shared Services
Network monitoring	Network activity monitoring	Security Operations Center (SOC)
Intrusion detection system	Malicious activity monitoring	SOC
Physical access (Badges)	Identification badges	SOC
Security infrastructure	Information systems security tools	SOC
Backups	Digital media backups and Enterprise-level backup, recovery, and storage services	Computing Infrastructure and Services
Directory services (Active Directory and supporting services)	Authentication and authorization	Computing Infrastructure and Services
Email (Office 365)	Email	Computing Infrastructure and Services
SQL servers: SQL databases	SQL infrastructure and services	Computing Infrastructure and Services
Storage	Data storage	Computing Infrastructure and Services
Virtual machine environment	Virtual machine infrastructure	Computing Infrastructure and Services
Windows Servers operating platform	Windows servers operating platform	Computing Infrastructure and Services
Oracle database	Oracle database	Enterprise Data Services
Oracle middleware	Oracle middleware	Enterprise Data Services
Unix	Variety of physical and virtual servers (HP, Sun, Oracle) and Operating Systems (Linux, Solaris)	Enterprise Data Services
Distributed Denial of Service (DDoS) protection	Distributed Denial of Service (DDoS) protection	Network and Voice Services
Network core	Redundant core	Network and Voice Services
Network services	Switches, routers, etc.	Network and Voice Services

Information Asset/Service	Description	Owner
Voice services	Analog telephony	Network and Voice Services
Voice over IP (VoIP)	Digital telephony	Network and Voice Services
Wireless	Wireless networking	Network and Voice Services
Domain Name Service (DNS)	Domain name – IP mapping	Network Security
Remote access/Virtual Private Network (VPN)	Secure remote access	Network Security
Reverse Proxy	Reverse proxy	Network Security
Web Application Firewall (WAF)	Filter, monitor, and block HTTP traffic	Network Security