



**State of Maine**  
**Department of Administrative & Financial Services**  
**Office of Information Technology**

---

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

---

## Table of Contents

Table of Contents.....	2
1.0 Document Purpose:.....	3
2.0 Scope: .....	3
3.0 Policy Conflict: .....	3
4.0 Roles and Responsibilities: .....	3
5.0 Management Commitment: .....	4
6.0 Coordination Among Agency Entities:.....	4
7.0 Compliance: .....	5
8.0 Procedures: .....	5
9.0 Document History and Distribution:.....	13
10.0 Document Review: .....	14
11.0 Records Management: .....	14
12.0 Public Records Exceptions: .....	14
13.0 Definitions: .....	14
Appendix A – Office of Information Technology Infrastructure Components/Services.....	16

## **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*. This is an important part of our overall security program that is focused on protecting the *confidentiality*, *integrity*, and *availability* of state information assets.

## **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 the State network.

## **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 are responsible for:**

4.1.1 Managing agency data in a secure manner.

4.1.2 Ensuring that any contracts for vendor hosted/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 Ensuring agency personnel are aware of all applicable penalties for non-compliance.

4.1.4 Developing and implementing agency-level policy and procedures, to meet any additional, pertinent system and information integrity statutory requirements.

### **4.2 Office of Information Technology (OIT):**

4.2.1 **The Office of Information Technology (OIT) is responsible for:**

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

- 4.2.1.1 Assigning an owner (identified in Appendix A) for each infrastructure component (e.g., network, firewall) supported by the Office of Information Technology (OIT).

### 4.2.2 OIT Component Owners are responsible for:

- 4.2.2.1 Ensuring that systems and information integrity protections are in place for their assigned component(s).
- 4.2.2.2 Implementing security directives.
- 4.2.2.3 Protecting information system memory from unauthorized code execution.
- 4.2.2.4 Utilizing standard operating procedures to manage required changes.
- 4.2.2.5 Utilizing integrity verification tools to detect unauthorized changes to software and information.

### 4.2.3 Information Security Office is responsible for:

- 4.2.3.1 Identifying and reporting information system flaws.
- 4.2.3.2 Performing scheduled information system security scans.
- 4.2.3.3 Protecting information systems from malicious code.
- 4.2.3.4 Monitoring information systems.

## 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:

The Office of Information Technology (OIT) provides system information and integrity at the enterprise-level for infrastructure consumed by agency information systems. Agencies coordinate with their Office of Information Technology (OIT) account managers, application development managers, and/or client technologies support staff to address any additional agency-specific system and information integrity requirements. Application development managers serve as the component 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 any violations.

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

## **8.0 Procedures:**

8.1 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.

### **8.2 Flaw Remediation (SI-2 including CE-1, CE-2):**

8.2.1 Agencies must ensure that appropriate mechanisms are in place to identify, report, and correct flaws in agency information systems.

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

8.2.1.1.1 Subscribes to Multi-State Information Sharing and Analysis Center (MS-ISAC) alerts and MITRE Common Vulnerabilities and Exposures (CVE) updates and notifications.

8.2.1.1.2 Distributes alerts, updates, and notifications to component owners.

8.2.1.1.3 Scans information systems at set intervals (weekly and monthly).

8.2.1.1.4 Reviews reports.

8.2.1.2 OIT Component Owners take the following actions to correct information system flaws:

8.2.1.2.1 Conduct security testing in accordance with deployment certification procedures.

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

- 8.2.1.2.2 Install operating system patches and hot fixes.
- 8.2.1.2.3 Install relevant security patches.
- 8.2.1.2.4 Utilize support and maintenance contracts to engage vendors to correct identified flaws in off the shelf software or firmware.
- 8.2.1.3 OIT Component Owners utilize standard operating procedures to manage change. They must:
  - 8.2.1.3.1 Use the centrally managed Office of Information Technology (OIT) Change Advisory Board (CAB) for change management.
    - 8.2.1.3.1.1 Production changes must follow the Office of Information Technology (OIT) [Change Management Policy](#)<sup>1</sup>.
  - 8.2.1.3.2 Install security-relevant software and firmware at defined intervals:
    - 8.2.1.3.2.1 The Information Security Office ensures that anti-virus .dat files are updated daily.
    - 8.2.1.3.2.2 Component Owners install patches at predefined intervals for the components they manage (e.g., security patches for hosting environments).
    - 8.2.1.3.2.3 Component Owners install patches, hot fixes and service packs, as necessary, to address specific issues (e.g., identified critical vulnerabilities), that cannot wait for the next scheduled cycle.
      - 8.2.1.3.2.3.1 This determination is made in collaboration with the Information Security Office.
      - 8.2.1.3.2.3.2 Interim compensating controls, approved by the Information Security Office, may alternatively

---

<sup>1</sup> <https://www.maine.gov/oit/policies/ChangeManagementPolicy.pdf>

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

be employed to address identified vulnerabilities.

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

### **8.3 Malicious Code Protection (SI-3 including CE-1, CE-2):**

- 8.3.1 Agencies must ensure that malicious code protections are in place to detect and eradicate malicious code at agency information system entry and exit points.
  - 8.3.1.1 OIT Component Owners implement malicious code protections at entry and exit points for the components they are responsible for.
    - 8.3.1.1.1 E.g., Network Services utilizes firewalls to perform real-time scans at network entry and exit points to detect and eradicate malicious code.
  - 8.3.1.2 OIT Component Owners keep malicious code protection mechanisms current by implementing new product releases when they become available.
    - 8.3.1.2.1 OIT Component Owners determine whether to update malicious code protections, automatically or manually.
  - 8.3.1.3 The Information Security Office employs products at information system entry and exit points to detect and eradicate malicious code.
  - 8.3.1.4 The Information Security Office ensures anti-virus .dat 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.
  - 8.3.1.5 The Information Security Office configures products to block malicious code, quarantine malicious code, and alert the Information Security Office, in response to malicious code detection.
  - 8.3.1.6 The Information Security Office team reviews quarantined code for potential information system impact, and, if appropriate, sends to the vendor for further analysis.

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

8.3.1.7 Quarantines are adjusted based on the risk level of the finding (e.g., considering false positives identified during analysis).

8.3.2 The Office of Information Technology (OIT) manages malicious code protection, centrally, at the enterprise-level as follows:

8.3.2.1 The Information Security Office and OIT Component Owners plan, implement, assess, authorize, and monitor malicious code protection products.

8.3.2.2 The Information Security Office consumes the Multi-State Information Sharing and Analysis Center (MS-ISAC) as a resource to plan, implement, assess, authorize, and monitor Albert.

### **8.4 Information System Monitoring (SI-4 including CE-1, CE-2, CE-4, CE-5, CE-7, CE-14):**

8.4.1 Agencies must ensure that their agency information systems are monitored to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections.

8.4.2 In accordance with the above, the Office of Information Technology performs the following information system monitoring:

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

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

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

8.4.2.4 OIT Component Owners perform information system monitoring for the components they are responsible for. E.g., Network Services employs firewalls to detect attacks and indicators of potential attacks, as well as unauthorized local, network, and remote connections.

8.4.2.5 The Information Security Office and Component Owners protect information obtained from intrusion monitoring tools from

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

unauthorized access, modification, and deletion by requiring team administrator credentials.

8.4.2.5.1 Access to this information must be granted based on the principle of least privilege.

8.4.3 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 source of information. Heightened activity may include any of the following actions, based on the Information Security Office assessment of the situation:

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

8.4.3.2 The Information Security Office and/or Component Owners leverage additional external incident response resources.

8.4.3.3 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.

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

8.4.5 Network Services employs intrusion detection/intrusion prevention (IDS/IPS) on network entry to detect attempted intrusions into the enterprise.

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

8.4.6 Network Services additionally employs firewall intrusion detection/intrusion prevention (IDS/IPS).

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

8.4.8 The Network Services team employs access points and wireless LAN controllers for over the air detection and reporting.

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

8.4.9 The Information Security Office and OIT Component Owners employ systems that alert teams when indications of compromise or potential compromise occur.

8.4.9.1 Automated mechanisms are employed, where available, to alert security personnel of unusual or inappropriate activities with security implications. Manual mechanisms are utilized in instances where automatic mechanisms are not implemented.

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

### **8.5 Security Alerts, Advisories, and Directives (SI-5):**

8.5.1 Agencies must 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.

8.5.1.1 The Information Security Office team receives and disseminates system security alerts, advisories and directives on an ongoing basis from multiple sources, including:

8.5.1.1.1 Multi-State Information Sharing and Analysis Center (MS-ISAC) emails

8.5.1.1.2 Albert suspicious internet traffic report

8.5.1.1.3 The Department of Homeland Security (DHS)

8.5.2 The Information Security Office generates internal security alerts, advisories, and directives as deemed necessary (e.g., in response to a known issue, a known threat, or to strengthen the state's security posture).

8.5.2.1 The audience for the communication is determined based on the nature of the alert, advisory, or directive (e.g., technical, agency end user, agency leadership).

8.5.2.1.1 Agency communication is coordinated through the Office of Information Technology (OIT) Account Managers, or Application Development Managers.

8.5.2.1.2 OIT technical communication is handled directly by the Information Security Office.

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

8.5.2.1.2.1 The Information Security Office establishes security directive implementation timeframes and notifies OIT Component Owners as part of the communication.

### 8.6 **Security Function Verification (SI-6):**

8.6.1 Agencies must ensure that mechanisms are in place to verify the correct operations of organizationally defined security functions that are pertinent to their agencies information systems.

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

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

8.6.1.1.1.1 Agencies collaborate with their Application Development Managers and/or Account Managers to implement supplemental security functions for OIT-supported agency information systems.

8.6.1.2 The Information Security Office works with Component Owners (typically system administrators) to review and verify configuration settings and deployment certifications to ensure security functions are implemented.

8.6.1.3 On a scheduled basis (frequency determined by the Component Owner, in collaboration with the Information Security Office), Component Owners conduct patching and verification.

8.6.1.4 If there is a failed security test, the Information Security Office notifies/works with Component Owners to address identified issues.

8.6.1.5 The Component Owner takes necessary action to address any identified issues (e.g., shut down or restart the component, etc.).

### 8.7 **Software, Firmware, and Information Integrity (SI-7 including CE-7):**

8.7.1 Agencies must ensure that integrity verification tools are employed, for agency information systems, to detect unauthorized changes to software and information.

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

- 8.7.1.1 OIT Component Owners utilize integrity verification tools to detect unauthorized changes to software and information (e.g., network, and security infrastructure tools).
- 8.7.1.2 The Information Security Office conducts integrity scans of information systems, on an as-needed basis, to reassess the integrity and software of information.
- 8.7.1.3 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.

### **8.8 SPAM Protection (SI-8 including CE-1, CE-2):**

- 8.8.1 Agencies must ensure that spam protection mechanisms are employed at agency information system entry and exit points to detect and act on unsolicited messages.
  - 8.8.1.1 OIT Component Owners employ spam protections, in accordance with the above, for the components that they manage.
  - 8.8.1.2 E.g., the Computing Infrastructure and Services team employs a centrally managed spam solution, that is automatically updated, to detect and act on unsolicited email messages.

### **8.9 Information Input Validation (SI-10):**

- 8.9.1 Agencies must 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.
  - 8.9.1.1 Agencies define the information inputs subject to this validation.
  - 8.9.1.2 OIT Application Development Managers ensure their teams implement input validation mechanisms for their assigned agency systems, in accordance with the above.
  - 8.9.1.3 The Information Security Office validates the implementation through regular application vulnerability scanning.

### **8.10 Error Handling (SI-11):**

- 8.10.1 Agencies must 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.

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

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

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

8.10.1.3 OIT Application Development Managers ensure that their teams implement error messages, in accordance with the above, for their assigned agency systems.

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

### 8.11 Information Handling and Retention (SI-12):

8.11.1 Agencies must ensure that agency information system information output is handled and retained in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.

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

8.11.1.2 The Office of Information Technology Component Owners implement agency-defined information handling and retention standards for the components that they manage (e.g., backup and recovery).

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

### 8.12 Memory Protection (SI-16):

8.12.1 Agencies must ensure that security safeguards are employed to protect information system memory from unauthorized code execution.

8.12.1.1 The Information Security Office employs malicious code protection products to protect information system memory from unauthorized code execution.

## 9.0 Document History and Distribution:

Version	Revision Log	Date
<i>Version 1.0</i>	<i>Version 1.0</i>	<i>July 19, 2019</i>

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

Approved by: Chief Information Officer

Legal Citation: [Title 5, Chapter 163: Office of Information Technology](#)<sup>2</sup>.

Waiver Process: [See the Waiver Policy](#)<sup>3</sup>.

### **Distribution**

This document will be distributed to all appropriate State of Maine personnel and will be posted on the OIT website (<https://www.maine.gov/oit/policies>).

### **10.0 Document Review:**

This document is to be reviewed annually and when substantive changes are made to policies, procedures or other authoritative regulations affecting this document.

### **11.0 Records Management:**

Office of Information Technology 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 three (3) years and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

### **12.0 Public Records Exceptions:**

Under the Maine Freedom of Access Act, 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 Legislature or, in the case of a political or administrative subdivision, to municipal 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:** Ensuring timely and reliable access to and use of information.  
Source: [NIST CSRC Glossary](#)<sup>4</sup>.

---

<sup>2</sup> <http://legislature.maine.gov/statutes/5/title5ch163sec0.html>

<sup>3</sup> <http://www.maine.gov/oit/policies/waiver.pdf>

<sup>4</sup> <https://csrc.nist.gov/glossary>

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

- 13.2 **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Source: [NIST CSRC Glossary](#)<sup>4</sup>.
- 13.3 **Information Asset:** Business applications, system software, development tools, utilities, hardware, infrastructure, etc.
- 13.4 **Integrity:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Source: [NIST CSRC Glossary](#)<sup>4</sup>.
- 13.5 **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.

**Appendix A – Office of Information Technology Infrastructure  
Components/Services**

<b>Component/Service</b>	<b>Description</b>	<b>Owner</b>
<b>Business Applications</b>	OIT developed applications to support specific business functions.	Application Development
Network monitoring	Network activity monitoring	Information Security Office (Infrastructure)
Intrusion Detection System (IDS)	Malicious activity monitoring	Information Security Office (Infrastructure)
Physical Access (Badges)	Identification badges	Information Security Office (Infrastructure)
Security Infrastructure	Information systems security tools	Information Security Office (Infrastructure)
Backups	Digital media backups	Computing Infrastructure and Services
Directory services (Active Directory and supporting servers)	Authentication and authorization	Computing Infrastructure and Services
Email (O365)	Email	Computing Infrastructure and Services
File and print	Enterprise-level backup, recovery and storage services.	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 (VM) environment	Virtual Machine (VM) 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

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

<b>Component/Service</b>	<b>Description</b>	<b>Owner</b>
Unix	Variety of physical and virtual servers (HP, Sun, Oracle) and Oss (Linux, Solaris)	Enterprise Data Services
Distributed Denial of Service (DDoS) protection	Distributed Denial of Service (DDoS) protection	Network Services
Network core	Redundant core	Network Services
Network services	Switches, routers, etc.	Network Services
Voice services	Analog telephony	Network Services
Voice over IP (VoIP)	Digital telephony	Network Services
Wireless	Wireless networking	Network Services
Domain Name Service (DNS)	Domain name – IP mapping	Network Services (Perimeter)
Remote access/Virtual Private Network (VPN)	Secure remote access	Network Services (Perimeter)
Reverse Proxy	Reverse proxy	Network Services (Perimeter)
Web Application Firewall (WAF)	Filter, monitor, and block HTTP traffic	Network Services (Perimeter)