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

System and Communications Protection Policy and Procedures (SC-1, SC-7, and SC-8)

Table of Contents

1.0. Purpose

The purpose of this document is to outline the State of Maine's policy and procedures for the protection of Agency information systems and their communications. This corresponds to the System and Communications Protection (SC) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Revision 4)[1].

2.0. Scope

2.1. This document applies to:

2.1.1. All State of Maine personnel, both employees and contractors;

2.1.2. Executive Branch Agency information assets, irrespective of location; and

2.1.3. Information assets from other State government branches that use the State network.

3.0. Conflict

If this document 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. Agency Management:

4.1.1. Ensures this Policy and Procedures are enforced.

4.2. Chief Information Security Officer:

4.2.1. Owns, executes, and enforces this Policy and Procedures.

4.2.2. Implements security policies, standards, and controls.

4.3. IT Procurement:

4.3.1. In collaboration with Agency Business Partners and Office of Information Technology (OIT) Information Asset Owners, holds all vendors/partners for externally hosted information assets accountable to this Policy and Procedures, within the vendor/partner's span-of-control.

4.4. Application Development Teams:

4.4.1. Maintain data flow diagrams.

4.5. OIT Computing Infrastructure and Services:

4.5.1. In collaboration with OIT Enterprise Data Services, ensures enhanced protections are implemented to maintain the integrity and confidentiality of information.

4.6. OIT Enterprise Data Services Team:

[1] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

4.6.1. In collaboration with OIT Computing Infrastructure and Services, ensures enhanced protections are implemented to maintain the integrity and confidentiality of information.

4.7. OIT Information Asset Owner:
4.7.1. Complies with this Policy and Procedures.

4.8. OIT Information Security Office:
4.8.1. Protects the State's information systems and assets against cybersecurity threats and vulnerabilities.
4.8.2. Reviews all security logs and reports exceptions to appropriate OIT teams.

4.9. OIT Network Services:
4.9.1. Maintains, manages, and protects all communication through the State of Maine data networks, including voice and wireless networks.
4.9.2. Implements preventative physical and software measures to protect State of Maine networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.

4.10. State of Maine Personnel:
4.10.1. Ensure State data is being stored only on OIT-approved devices, computers, and media.

5.0. Management Commitment

The State of Maine is committed to following this document.

6.0. Coordination Among Agency Entities

OIT coordinates system and communication protections with Agencies to ensure the security of State of Maine information assets in accordance with Title 5, Chapter 163 §1971-1985[2]. Agencies and OIT coordinate to meet all state and Federal audit documentation and reporting compliance requirements.

7.0. Compliance

7.1. For State of Maine employees, failure to comply with this document 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 contractors will be notified of any violations.
7.3. Individuals and Agency Leads 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.

[2] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

8.0. Procedures

8.1. SC Controls – Cross References Coming Soon:

8.1.1. The following controls for the System and Communications Protection Policy and Procedures (SC) will be published in separate policy documents:

8.1.1.1. System and Communications Protection Procedures for Defense in Depth (SC-2, 4, 5, 20, 21, 22, 23, 28, 32, 39);

8.1.1.2. System and Communications Protection Procedures for Encryption Mechanisms (SC-12, 13, 17); and

8.1.1.3. System and Communications Protection Procedures of Specific Technologies ([Network SC-6, 10], [Collaborative Devices SC-15], [VOIP SC-19], [Mobile Devices SC-18], and [Wireless SC-40]).

8.2. The procedures listed below are designed to satisfy the security control requirements of this Policy (SC-1, SC-7, and SC-8) as outlined in NIST Special Publication 800-53 (Revision 4), Internal Revenue Service (IRS) Publication 1075, Centers for Medicare & Medicaid Services (CMS) Acceptable Risk Safeguards 3.1, Criminal Justice Information Services (CJIS) Security Policy, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and to satisfy Federal law.

8.3. **Boundary Protection (SC-7)**

8.3.1. Agency Partners, in collaboration with OIT:

8.3.1.1. Connect to external networks or information systems (see Definitions) only through managed interfaces (see Definitions) consisting of boundary protection devices (see Definitions) arranged in accordance with statewide security architecture requirements (see the General Architecture Principles[3]). Managed interfaces include, for example, gateways, routers, firewalls, network-based malicious code analysis, and virtualization systems, or encrypted tunnels implemented within the security architecture (e.g., routers protecting firewalls or application gateways). See the Access Control Procedures for Users Policy, AC-2[4].

8.3.2. OIT Information Asset Owners:

8.3.2.1. Protect the confidentiality and integrity of the information being transmitted across each interface in accordance with the Data Exchange Policy[5].

8.3.3. OIT Network Security Team:

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/general-architecture-principles_1.pdf
[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/access-control-procedures-for-users.pdf
[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/data-exchange-policy.pdf

8.3.3.1. Monitors and controls communications at the external boundary of information systems and at key Agency-chosen internal boundaries within the system.

8.3.3.1.1. External boundaries are monitored and controlled through the perimeter firewall.

8.3.3.1.2. Key Agency-chosen internal boundaries are monitored and controlled through the Data Center Firewalls and network segmentation tools.

8.3.3.2. Implements subnetworks ("subnets") (see Definitions) using Virtual Local Area Networks for publicly accessible system components that are physically and logically separated from internal agency network.

8.3.4. **Boundary Protection Access Points (SC-7(3)):**

8.3.4.1. The OIT Network Security Team limits the number of external network connections to information systems using the following methods and technologies:

8.3.4.1.1. Circuit management;

8.3.4.1.2. Firewall implementation including a Web Application Firewall with Distributed Denial-of-Service infrastructure;

8.3.4.1.3. Firewall rule sets;

8.3.4.1.4. Site-to-Site, user-based Virtual Private Network (VPN);

8.3.4.1.5. Intrusion Detection System;

8.3.4.1.6. Intrusion Prevention System; and

8.3.4.1.7. Active Directory groups.

8.3.5. **Boundary Protection External Telecommunications Services (SC-7(4)):**

8.3.5.1. The OIT Network Security Team:

8.3.5.1.1. Implements a managed interface for each external telecommunication service (see Definitions) to ensure all internet and foreign, untrusted partner, networks are segregated onto separate firewall interfaces.

8.3.5.1.2. Establishes a traffic flow policy for each managed interface.

8.3.5.1.2.1. From time to time, the Information Security Office, at its discretion, reviews exceptions to the traffic flow policy. Traffic flow reviews also work with the application development teams to update data flow diagrams to meet

federal compliance requirements (e.g., Federal Tax, Social Security, Criminal Justice, Affordable Care Act data).

8.3.5.1.2.2. Exceptions that are no longer supported by an explicit mission/business need are removed.

8.3.6. **Boundary Protection Deny by Default/Allow by Exception (SC-7(5)):**

8.3.6.1. The OIT Network Security Team establishes information systems at managed interfaces to deny network communications traffic by default, and allow network communications traffic by exception (i.e., deny all, permit by exception).

8.3.6.1.1. This applies to the inbound network communications traffic to ensure only those connections which are essential and approved by the Chief Information Security Officer (CISO) are allowed.

8.3.6.1.2. For outbound traffic, the CISO reviews and bans traffic by exception.

8.3.7. **Boundary Protection Host-Based Protection (SC-7(12)):**

8.3.7.1. The OIT Network Security Team implements host-based boundary protection mechanisms to separate information system components supporting missions and/or business functions including:

8.3.7.1.1. Restricting rogue devices (see Definitions) from manipulating the State's routing tables.

8.3.7.1.2. Implementing a firewall authentication mechanism (see Definitions) to provide accountability for the individual and to ensure device configuration does not become corrupted with false entries.

8.3.7.1.3. Screening internal network addresses from external view.

8.3.7.1.4. Configuring local user accounts on network firewalls, to eliminate possible extended outages.

8.3.7.1.4.1. Local accounts are configured to only be used when the device cannot contact the central unit.

8.3.7.1.4.2. During normal operation, the local account exists, but is not used.

8.3.7.1.5. Keeping passwords for firewalls in a secure encrypted form (see Identification and Authentication Policy and Procedures[6] (IA-1), intranet only).

8.3.7.1.6. Limiting temporary or emergency port openings to no more than 31 days, at which time the port is closed, or additional hardening (see Definitions) is developed.

8.3.7.1.7. Implementing logging features on State network firewalls to capture all packets dropped or denied by the firewall.

8.3.7.1.7. From time to time, the Information Security Office, at its discretion, reviews State network firewall logs.

8.3.7.1.8. Implements firewall rule sets to always block the following types of network traffic:

8.3.7.1.8.1. Unauthorized scanning activity.

8.3.7.1.8.2. Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.

8.3.7.1.8.3. Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall.

8.3.7.1.8.4. Inbound network traffic containing IP Source Routing Information (see Definitions).

8.3.7.1.8.5. Inbound or outbound network traffic containing a source or destination address of 0.0.0.0 and/or containing directed broadcast addresses (see Definitions).

8.3.7.1.9. Installs firewalls in data center locations that are physically secure from tampering.

8.3.7.1.10. Restricts firewall configurations and associated documentation information to authorized personnel within the Network Security Team, including authorized administrators, auditors, and security oversight personnel.

8.3.8. **Boundary Protection Isolation of Security Tools (SC-7(13)):**

8.3.8.1. The OIT Network Security Team isolates boundary protection mechanisms from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

[6] http://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf

8.3.8.1.1. Network routing controls are implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal subnetworks.

8.3.8.1.2. Access points between Non-Protected systems (standard agency information systems or untrusted networks) and any system components in the protected agency information system are restricted.

8.3.8.1.2.1. OIT allows only inbound and outbound traffic to that which is necessary for the protected agency information system.

8.3.9. **Boundary Protection Fail Secure (SC-7(18)):**

8.3.9.1. The OIT Network Security Team implements fail secure mechanisms to ensure information systems fail closed (see Definitions) and to prevent information systems from entering into unsecure states in the event of an operational failure of a boundary protection device.

8.3.10. The following NIST publications are recommended as guidance for the specified information technology:

8.3.10.1. NIST SP 800-41, Revision 1[7] for firewalls and firewall rules.

8.3.10.2. NIST SP 800-189[8] for routers.

8.3.10.3. NIST SP 800-77[9] for VPNs.

8.3.10.4. NIST SP 800-94[10] for Intrusion Detection and Prevention Systems (IDPS).

8.4. **Transmission Confidentiality and Integrity (SC-8)**

8.4.1. The following procedures describe how OIT and Agency Business Partners ensure that information systems protect the confidentiality and integrity of transmitted information.

8.4.2. For OIT-controlled locations, OIT:

8.4.2.1. Implements safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions in accordance with the Telecommunications Facilities & Wiring Specifications[11] and industrial cabling standards.

[7] https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final
[8] https://csrc.nist.gov/publications/detail/sp/800-189/final
[9] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf
[10] https://csrc.nist.gov/publications/detail/sp/800-94/rev-1/draft
[11] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/wiring-specs.pdf

8.4.2.2. Ensures all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized personnel within OIT.
8.4.2.3. Ensures all telecommunication ("telco") closets are accessible only to authorized personnel within State agencies and OIT.

8.4.3. The OIT Network Services Team:
8.4.3.1. Uses network monitoring tools and capabilities to detect and monitor for suspicious network traffic.
8.4.3.2. Secures interfaces through network demarcation between agency-controlled and non-Agency controlled/public networks.
8.4.3.3. Implements standardized authentication mechanisms to:
8.4.3.3.1. Authenticate users through Active Directory; and
8.4.3.3.2. Authenticate devices using Active Directory, Multi-Factor Authentication, and identity/access controls.
8.4.3.4. Implements secure protocols, Secure Shell/Transport Layer Security (TLS) and Internet Protocol Security (IPSec), for secure network management functions to:
8.4.3.4.1. **Cryptographic or Alternate Physical Protection SC-8(1)**: Implement cryptographic mechanisms (see Definitions) to prevent unauthorized disclosure of information and to detect changes to information during transmission unless otherwise protected by alternative physical safeguards.
8.4.3.4.2. **Pre/Post Transmission Handling SC-8(2)**: Maintain the confidentiality and integrity of information during preparation for transmission and during reception.
8.4.3.5. Documents and retains on file a case-by-case risk management determination, for each type of confidential information, as to the appropriateness of its encrypted transmission to a party not served by the agency's internal network (see Data Exchange Policy[12]).
8.4.3.6. Ensures all communications that transfer Sensitive Data (TLP: Amber) and Restricted Data (TLP: Red) (see Data Exchange Policy) between web clients and web servers employ the most current secure-transport protocol that includes the most recent version of TLS.
8.4.3.7. Addresses the risk involved in the transfer of different types of data and implement safeguards through the means of exchange used, such as through email, the internet, or exchange of electronic media and portable media in accordance with the Data Exchange Policy.
8.4.3.8. Monitors for anomalies or known signatures via:
8.4.3.8.1. Intrusion detection systems;
8.4.3.8.2. Intrusion prevention systems; and
8.4.3.8.3. Network behavior analysis tools.

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

8.4.4. For OIT-hosted information assets, OIT Service Teams are responsible for the fulfillment of the items below under the direction of IT Directors. For remote-hosted information assets, the hosting partner is responsible for the fulfillment of the items below, with oversight from IT Procurement in collaboration with Agency business partners.

8.4.4.1. Ensures enhanced protection through the implementation of TLS and/or IPSec to maintain the integrity and confidentiality of information, including, but not limited to, the following types of transmissions:

8.4.4.1.1. Internal traffic within the information system and applications;
8.4.4.1.2. Internal traffic between two or more information systems;
8.4.4.1.3. External traffic to or across the internet;
8.4.4.1.4. Connections to cloud services and remote data centers;
8.4.4.1.5. Remote access;
8.4.4.1.6. Email;
8.4.4.1.7. FTP transmissions;
8.4.4.1.8. Web services;
8.4.4.1.9. Voice over Internet Protocol;
8.4.4.1.10. Audio and video to include video teleconferencing hardware, appliances and/or applications; and
8.4.4.1.11. Wireless client-to-host communications.

9.0. Document Details

9.1. Initial Issue Date: July 15, 2021
9.2. Latest Revision Date: July 15, 2021
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[13]
9.6. Waiver Process: Waiver Policy[14]
9.7. Distribution: Internet[15]

10.0. Review

This document will be reviewed annually, and whenever substantive changes are made to Policies, Procedures, or other authoritative regulations affecting this document.

[13] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[15] https://www.maine.gov/oit/policies-standards

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 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 (FOAA), 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. Authentication Mechanism: a mechanism that verifies user identities to ensure authorized persons can access the resources they need and to keep unauthorized persons from gaining access to resources (see Identification and Authentication Policy and Procedures[16] (IA-1), intranet only).

13.2. Boundary Protection Devices: devices that control the flow of information into or out of an interconnected system and/or monitor and control communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary-protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.

13.3. Cryptographic Mechanisms (Cryptographic Modules): any combination of hardware, firmware, or software that implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques, and random-number generation.

13.4. Directed Broadcast Address: a special Internet Protocol (IP) address used to transmit messages and data packets to network systems.

13.5. External Telecommunications Service: An external public switched telephone and communications, or external public switched non-telephonic service that offers either wired or wireless voice and data services over a large area.

[16] http://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf

13.6. Fail Closed: the practice of a device or system being set, through either physical or software enabled means, to shut down, preventing any further operation, when failure conditions are detected.

13.7. Hardening: a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas.

13.8. Information System (Information Asset): a discrete, identifiable piece of information technology, including hardware, software, firmware, systems, services, and related technology assets used to execute work on behalf of OIT or another State Agency. (NIST Special Publication (SP) 800-30).

13.9. IP Source Routing Information: information that allows the sender of a packet to specify which route the packet should take on the way to its destination and on the way back.

13.10. Managed Interfaces: a network interface dedicated to configuration and management operations.

13.11. Rogue Devices: unauthorized devices that are connected to a system but do not have permission to access and operate within the network.

13.12. Subnetwork: a logically segmented piece of a larger network.

14.0. Abbreviations

14.1. CISO Chief Information Security Officer
14.2. CJIS Criminal Justice Information Services
14.3. CMS Centers for Medicare & Medicaid Services
14.4. HIPAA Health Insurance Portability and Accountability Act
14.5. IDPS Intrusion Detection and Prevention Systems
14.6. IPSec Internet Protocol Security
14.7. IRS Internal Revenue Service
14.8. NIST National Institute of Standards and Technology
14.9. OIT Office of Information Technology
14.10. SC System and Communications Protection Policy and Procedures
14.11. TLS Transport Layer Security
14.12. URL Uniform Resource Locators
14.13. VPN Virtual Private Network