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

System and Communications Protection Procedures for Specific Technologies (SC-6, 10, 15, 18, 19)

System and Communications Protection Procedures for Specific Technologies (SC-6, 10, 15, 18, 19, and 40)

Table of Contents

System and Communications Protection Procedures for Specific Technologies (SC-6, 10, 15, 18, 19, and 40)

1.0. Purpose

The System and Communication Protection Procedures (SC) for Specific Technologies details State of Maine (SOM) procedures to leverage multiple layers of security measures to protect an organization's assets. The security controls detailed in this document align with select SC controls detailed in National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 4.

2.0. Scope

2.1. These procedures apply to all State of Maine personnel, both 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. Conflict

If these procedures conflict with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Procedures

4.1. SC Controls, Cross References: The following controls for the System and Communications Protection Policy and Procedures (SC) are published in separate policy and procedure documents:

4.1.1. System and Communications Protection Policy and Procedures (SC-1, 7, 8);[1]

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

4.1.3. System and Communications Protection Procedures for Encryption Mechanisms (SC-12, 13, and 17).[3]

4.2. Resource Availability (SC-6)

4.2.1. OIT protects the availability of on-premises hosted resources through the following safeguards:

4.2.1.1. For Linux servers, the OIT Enterprise Data Services team uses Linux Control Groups (Cgroups) to protect the availability of information system resources for multiple users.

4.2.1.1.1. Cgroups automate configurations to prioritize processes that prevent lower-priority processes from delaying or interfering with information systems that service higher priority processes.

4.2.1.1.2. Cgroups also establishes quotas to prevent users or processes from obtaining more than the predetermined amounts of resources.

---

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemCommunicationsProtectionPolicy.pdf

[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SCDefenseInDepthProcedures.pdf

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SCEncryptionMechanismsProcedures.pdf

4.2.1.2. For Oracle Databases, the OIT Enterprise Data Services protects the availability of on-premises hosted resources by:
- 4.2.1.2.1. Continuously monitoring all processes, memory utilization, and all characteristics of the platforms, and promptly following up on any unusual spikes.
- 4.2.1.2.2. Preassigning process-based memory usage on a per process basis. Memory is preassigned to processes uniformly in alignment with vendor recommendations.
- 4.2.1.2.3. Fine tuning, over time, preassigned memory allocations for processes based on discussions with consumers, process monitoring trends, etc.
- 4.2.1.2.4. Currently, there are no preexisting limits being implemented on Central Processing Unit (CPU) consumption.

4.2.1.3. For Oracle Middleware, the Enterprise Data Services team protects the availability of on-premises hosted resources by:
- 4.2.1.3.1. Configures resource limits through managed server memory, Java Virtual Machine (JVM), and connection configurations.
  - 4.2.1.3.1.1. In most cases, applications are provided with a dedicated JVM which allows for custom resource configurations.
  - 4.2.1.3.1.2. The Oracle Middleware team works with the application owners to determine a configuration that will sufficiently address the needs of the application.
  - 4.2.1.3.1.3. JVM and memory configurations are fine-tuned over time based on consumer needs.
- 4.2.1.3.2. Maintains isolated virtual machines (VM) for select agencies and applications.
  - 4.2.1.3.2.1. Segmentation is determined based on an application agency and/or application workload.
  - 4.2.1.3.2.2. The Oracle Middleware team ensures that JVMs are tuned, and the applications are functioning normally, from an infrastructure perspective.
  - 4.2.1.3.2.3. Agents and processes monitor the health of the infrastructure to allow for quick review and/or resolution of resource issues/concerns.

4.2.1.4. For Windows/SQL servers, the OIT Computing Infrastructure & Services team:
- 4.2.1.4.1. Segments servers by workload.
- 4.2.1.4.2. Advises Agencies against co-housing workloads on a single server to prevent resource contention.

4.2.1.4.3. Ensures only pre-approved software is installed on servers.
4.2.1.4.4. Restricts the installation of software to Server Administrations and Application Administrators who have approved and delegated access to the servers.
4.2.1.4.5. Ensures all software packages have known standard configurations and expected boundaries of operation for resource consumption.
4.2.1.4.6. Ensures all the operating parameters are optimized to maximize performance of SQL Server processes.
4.2.1.4.7. Restricts users from adding additional resources without first requesting them from the Computing Infrastructure & Services team.

4.2.2. For cloud-hosted resources, the OIT Cloud Center of Excellence works with cloud vendors to implement comparable best practices.

4.3. **Network Disconnect (SC-10)**

4.3.1. The OIT Network Services team ensures Virtual Private Network (VPN) connections associated with a communications session are:
4.3.1.1. Terminated at the end of a session when the user disconnects.
4.3.1.2. Automatically deallocate inactive Dynamic Host Configuration Protocol (DHCP) (see Definition) leases after seven (7) days. An active Internet Protocol (IP) addressed may be reallocated as long as the device is in session.
4.3.1.3. Automatically terminated thirty (30) minutes after the computer enters sleep mode due to inactivity.
4.3.1.4. Automatically terminated after 24 hours of continuous connection.
4.3.1.5. Terminated or suspended upon issuance of an order by the OIT Chief Information Officer (CIO) or Chief Information Security Officer (CISO).

4.3.2. Following all session terminations, authentication is required for the user to reenter the SOM network.

4.4. **Collaborative Computing Devices (SC-15)**

4.4.1. OIT Client Technologies prohibits remote activation of collaborative computing devices (see Definitions), for example, networked white boards, cameras, and microphones.
4.4.2. OIT Client Technologies provides explicit indication of use to users physically present at the collaborative computing devices. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.
4.4.3. **Physical Disconnect (SC-15(1)):** OIT Client Technologies ensures collaborative computing devices are automatically disconnected when a session ends to ensure participant disconnection.

4.4.4. **Disabling/Removal in Secure Work Areas (SC-15(3)):** OIT Client Technologies disables remote access to collaborative computing devices from information systems or information system components through VPN Deny and Active Directory to prevent, for example, eavesdropping on conversations.

4.4.5. **Explicitly Indicate Current Participants (SC-15(4)):** Signaling local users is done to show those who are physically present at their cameras when collaborative computing devices are in use.

4.5. Mobile Code (SC-18)

4.5.1. OIT Security, as well as all the Information Asset Owners, define and establish usage, restrictions, and guidance for mobile code technologies (see Definitions). They authorize, monitor, and control mobile code technologies within the information system through OIT's Change Management Policy and Procedures.[4]

4.5.2. The most current state-of-the-art mobile code technologies are derived from principally two sources: the product vendors and other Industry Partners (see Definitions).

4.5.3. When mobile code technologies are identified as either deprecated and/or vulnerable, these products are processed through the procedures outlined in OIT's Change Management Policy and Procedures[5] for divestment.

4.6. Voice Over Internet Protocol (SC-19)

4.6.1. OIT Voice Services establishes usage restrictions, and implementation guidance for Voice over Internet Protocol (VoIP) technologies through the following:

4.6.1.1. Session Border Controllers (SBC) (see Definitions) separated by a demilitarized zone (DMZ) allow access to the Public Switched Telephone Network (PSTN) from the State of Maine.

4.6.1.1.1. The SOM SBC is cabled directly to the PSTN service provider's SBC for security.

4.6.1.2. All SOM voice core systems, traffic, and equipment reside in a VoIP-dedicated virtual local area network (VLAN) subnet with isolated and reserved IP addresses.

4.6.1.2.1. Every device on the VLAN subnet must present their own certificate.

4.6.1.2.2. All phones use certificates based in the firmware.

4.6.1.3. Access to SOM networks, including VoIP resources, is controlled by firewalls.

4.6.1.4. All physical and soft phones are configured to use Security Sockets Layer (SSL) to connect to the core system.

[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf
[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf

4.6.1.5. All core equipment is housed in secure rooms with access limited to only approved personnel who have completed background checks and necessary training.

4.6.1.6. Implementation guidance is provided through both documentation and internally created training videos.

4.6.2. OIT Voice Services authorizes, monitors, and controls the use of VoIP within the State of Maine through the following methods:

4.6.2.1. Authorized Telco Coordinators are responsible for approving any user requests to use VoIP services within the SOM.

4.6.2.2. Agency Telco Coordinators authorize new employees, pay VoIP bills, and completely monthly audits on the number of lines in their agency.

4.6.2.3. The SOM's contracted service provider for VoIP monitors the services for suspicious activity.

4.6.2.3.1. The contracted service provider alerts the Voice Services team immediately if suspicious activity/behavior is detected.

4.6.2.3.2. The contracted service provider will shut down any services where suspicious activity has been detected.

4.6.2.4. Core VoIP systems are monitored by the OIT Information Security Office using Splunk.

4.6.2.5. Syslog servers log system events and maintain security and access logs.

4.6.2.6. Security, access, and billing logs are reviewed regularly for unusual activity.

5.0. Document Details

5.1. Initial Issue Date: November 13, 2024
5.2. Latest Revision Date: November 13, 2024
5.3. Point of Contact: Enterprise.Architect@Maine.Gov
5.4. Approved By: Chief Information Officer, OIT
5.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[6]
5.6. Waiver Process: Waiver Policy[7]
5.7. Distribution: Internet[8]

6.0. Review

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

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

7.0. Records Management

OIT major policies and procedures fall under Maine State Archives General Schedule 1, Administrative Records[9], series GS1.13a, Policies and Procedures – Major. They will be retained for 6 years after being superseded or withdrawn. Typically, these records are archival (permanent) value, and will be evaluated on a case-by-case basis by Maine State Archives staff. If deemed archival (permanent) value, then OIT should send these records to Maine State Archives for their historical/research collection.

8.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA), certain public records exceptions may limit disclosure of OIT 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.

9.0. Definitions

9.1. Certificate Authority: A trusted entity that issues and revokes public key certificates. Source: NIST.[10]

9.2. Collaborative Computing Devices: Technology that allows people in geographically distant locations to work together. Collaborative computing devices include, for example, networked white boards, cameras, and microphones.

9.3. Dynamic Host Configuration Protocol (DHCP): A client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

9.4. Industry Partner: An external party that apprises OIT Information Security of the cybersecurity-vulnerability landscape. These can be open-channel partners such as product vendors, trade magazines, security research organizations, and so on; or they can be closed-channel partners, such as the Multi-State Information Sharing and Analysis Center and the Maine Information and Analysis Center.

9.5. Mobile Code Technologies: Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript). Source: NIST.[11]

[9] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf
[10] https://csrc.nist.gov/glossary/term/certificate_authority
[11] https://csrc.nist.gov/glossary/term/mobile_code_technologies

9.6. Session Border Controllers: A network function which secures VoIP infrastructures while providing interworking between incompatible signaling messages and media flows (sessions) from end devices or application servers. Session Border Controllers are typically deployed at both the network edge and at carrier interconnects, the demarcation points (borders) between their users and other service providers. Source: metaswitch[12]

9.7. Voice Over Internet Protocol (VoIP): A term used to describe the transmission of packetized voice using the IP and consists of both signaling and media protocols. Source: NIST.[13]

10.0. Abbreviations

10.1. DHCP: Dynamic Host Configuration Protocol
10.2. FOAA: Freedom of Access Act (Maine)
10.3. IP: Internet Protocol
10.4. NIST: National Institute of Standards and Technology
10.5. OIT: Office of Information Technology
10.6. SC: System and Communications Protection Policy and Procedures
10.7. SSID: Service Set Identifier
10.8. VoIP: Voice Over Internet Protocol

[12] https://www.metaswitch.com/knowledge-center/reference/what-is-a-session-border-controller-sbc
[13] https://csrc.nist.gov/glossary/term/voip