State of Maine
Department of Administrative and Financial Services
Office of Information Technology (OIT)

Security Planning Policy and Procedures (PL-1)

Table of Contents

1.0. Purpose

The purpose of this document is to outline the Office of Information Technology's (OIT's) policy and procedures for security planning. This document corresponds to the Security Planning Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).[1]

2.0. Scope

2.1. This document applies to:

2.1.1. All State of Maine personnel, both employees and contractors with access to Executive Branch information assets, irrespective of location, or information assets from other State government branches that use the State network;

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 Business Partners

4.1.1. Cooperate with OIT Information Security to develop system security plans.

4.1.2. Develop and implement agency-level policy and procedures to meet additional statutory requirements or agency-specific controls.

4.1.3. Ensure that personnel comply with information security training requirements and are trained in and agree to the Rules of Behavior (PL-4).[2]

4.2. OIT Information Asset Owners

4.2.1. Comply with this Security Planning Policy and Procedures document.

4.3. OIT Information Security

4.3.1. Owns, executes, and enforces this Security Planning Policy and Procedures.

5.0. Management Commitment

The State of Maine is committed to following this document.

6.0. Coordination Among Agency Entities

OIT assists agencies in the development of the required system security plans and in meeting their information security architecture needs. Additionally, as required by statute, OIT establishes and maintains the minimum Rules of Behavior[3] for information system (see Definitions) users. Agencies may add requirements to the

[1] https://nvd.nist.gov/800-53/Rev4/control/PL-4
[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf
[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf

Rules of Behavior to meet specific agency needs but cannot remove requirements as established by OIT.

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 violations.

7.3. Personnel are also subject to any applicable 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

8.1. The following serve as the baseline procedures for security planning requirements. For information assets under its purview, OIT does the following:

8.2. System Security Plan and Concept of Operations (PL-2)

8.2.1. OIT Information Security assists the agencies (and vendors) in the development of System Security Plans (SSPs) to meet Federal regulatory requirements and as otherwise required.

8.2.2. OIT subscribes to a security architecture using NIST SP 800-53 security control and control enhancements. The collective body of all plans, policies, and procedures that documents each NIST control family (e.g., Access Control, Planning, Security Assessments) acts as the enterprise level System Security Plan.

8.2.3. OIT assists Maine Department of Health and Human Services (DHHS) Office of Family Independence to develop an SSP and comply with the mandates of the Patient Protection and Affordable Care Act of 2010, as determined by the Centers for Medicare and Medicaid Services.

8.2.4. OIT also assists the following agencies that receive Federal Taxpayer Information (FTI) (see Definitions) in the preparation of their respective SSPs as determined by the Internal Revenue Services (IRS):

8.2.4.1. DHHS;

8.2.4.2. Maine Department of Labor (DOL), Bureau of Unemployment Compensation; and

8.2.4.3. Maine Department of Administrative and Financial Services Maine Revenue Services.

8.2.5. As outlined in IRS Publication 1075, Safeguards for Protecting Federal Tax Returns and Return Information, an approved and accurate Safeguard Security Report (SSR) satisfies the requirement of the SSP. The SSR is required to be submitted to the IRS annually by May 30th.

8.2.6. OIT Assists DHHS and DOL with the completion of the Security Evaluation Questionnaire (SEQ) that is deemed an integral part of the compliance review process for the Social Security Administration. SEQs are required when there are changes to the data exchange and prior to on-site audits.

8.3. **Rules of Behavior (PL-4, including CE-1)**

8.3.1. The Rules of Behavior for Information Security Policy governs the individual behavior of personnel for the appropriate access to and use of State of Maine assets. See the Rules of Behavior (PL-4)[4] for more information.

8.4. **Information Security Architecture (PL-8, related to PM-7)**

8.4.1. OIT, in its General Architecture Principles,[5] outlines guidance to aid in everyday decision making that:

8.4.1.1. Describes the overall philosophy, requirements, and approach to be taken with regards to protecting the confidentiality, integrity, and availability of information. One of the eight principles established is that "Security and Privacy are foundational to everything else." The State implements security and privacy best practices at all levels of government to ensure the confidentiality, integrity, and availability of its information assets;

8.4.1.2. Describes how the information security architecture is integrated into and supports the enterprise architecture. OIT describes security in the General Architecture Principles as foundational;

8.4.1.3. Describes any information security assumptions about, and dependencies on, external services.

8.4.1.3.1. Another principle is that "The State is a single, unified enterprise." This principle is used to maximize resources and as a basis for effective disaster recovery.

8.4.1.3.2. The principle to "First reuse; then buy; then build", "Centralize Authentication; Federate Authorization", and "Be Cloud Smart" describe interdependency considerations. The principle of "Choose new products carefully" states that the top product selection criteria are cybersecurity, privacy, and accessibility.

8.4.2. Information security architecture is designed using a defense-in-depth approach which strategically allocates safeguards that operate in a coordinated and mutually reinforcing manner so that adversaries must overcome multiple safeguards to achieve their objective.

[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf
[5] https://www.maine.gov/oit/architecture/documents/GeneralArchitecturePrinciples.pdf

8.4.3. Security architecture for information systems is consistent with the OIT information security plans, policies, and procedures,[6] which establish the minimum benchmark and implements controls to protect State information assets from unauthorized use, disclosure, modification, and destruction, and to ensure the confidentiality, integrity, and availability of information assets.

8.4.3.1. OIT also implements NIST standards and controls into policy, with which the security architecture of information systems is compliant.

8.4.3.2. Other policies, including but not limited to the Network Device Management Policy,[7] the Remote Hosting Policy,[8] the User Device and Commodity Application Policy,[9] and Mobile Device Policy,[10] ensure the security of State information assets. All public OIT policies can be found at https://www.maine.gov/oit/policies/.

8.4.3.3. Any information system which is not compliant with OIT policies must go through a rigorous waiver process managed by Enterprise Architecture and Security and including other relevant subject matter experts in order to ensure the presence of compensating controls and confirm that that information system as well as all State of Maine information assets are secure and protected. See the Waiver Policy[11] for more information.

8.4.4. Enterprise Architecture, in collaboration with Security, Compliance, IT Procurement, and other relevant parties, vets all proposed new technologies and technology solutions in regard to security to ensure that new products and technologies align with the State of Maine's overall security architecture.

8.4.5. IT Procurement, in collaboration with Enterprise Architecture, Security, Compliance, and other relevant parties, vets all technology related procurement contracts – both new and renewed – through contract review to ensure that contracts align with the State of Maine's overall security architecture.

8.4.6. Information security architecture is updated as needed to reflect changes in enterprise architecture.

8.4.7. Acquisition-related documents and security plans are updated as needed to reflect changes in information security architecture.

9.0. Document Details

9.1. Initial issue Date: June 24, 2020

9.2. Latest Revision Date: June 30, 2021

---

[6] https://www.maine.gov/oit/policies/

[7] https://www.maine.gov/oit/policies/NetworkDeviceManagementPolicy.pdf

[8] https://www.maine.gov/oit/policies/RemoteHostingPolicy.pdf

[9] https://www.maine.gov/oit/policies/UserDeviceCommodityAppPolicy.pdf

[10] https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf

[11] https://www.maine.gov/oit/policies/waiver.pdf

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[12]
9.6. Waiver Process: Waiver Policy[13]
9.7. Distribution: Internet[14]

10.0. Review

This document will 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 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. Federal Taxpayer Information (FTI): Federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is received directly from the IRS (or obtained through an authorized secondary source), covered by the confidentiality protections of the Internal Revenue Code (IRC), and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight. FTI may contain personally identifiable information (PII) IRS Publication 1075.[15]

13.2. Information system: Used interchangeably with *information asset*. 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

[12] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[13] https://www.maine.gov/oit/policies/waiver.pdf
[14] https://www.maine.gov/oit/policies-standards
[15] https://www.irs.gov/pub/irs-pdf/p1075.pdf

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.

13.3. Personally Identifiable Information (PII): Information that can be used to distinguish or trace the identity of an individual (for example, name, social security number, biometric records, and so on) alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual (such as date and place of birth, mother's maiden name, and so on). It also includes personal information protected from disclosure under Federal or State privacy laws.[16]

14.0. Abbreviations

14.1. DHHS: Department of Health and Human Services
14.2. DOL: Department of Labor
14.3. FOAA: (Maine) Freedom of Access Act
14.4. FTI: Federal Taxpayer Information
14.5. IRC: Internal Revenue Code
14.6. IRS: Internal Revenue Service
14.7. NIST: National Institute of Standards and Technology
14.8. OIT: Office of Information Technology
14.9. SEQ: Security Event Questionnaire
14.10. SSP: System Security Plan
14.11. SSR: Safeguard Security Report

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