



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

---

**Security Planning (PL-1)**

---

# Security Planning (PL-1)

## Table of Contents

1.0.	Purpose.....	3
2.0.	Scope.....	3
3.0.	Policy Conflict.....	3
4.0.	Roles and Responsibilities .....	3
5.0.	Management Commitment.....	3
6.0.	Coordination Among Agency Entities.....	3
7.0.	Compliance.....	4
8.0.	Procedures .....	4
9.0.	Document Details.....	6
10.0.	Review.....	7
11.0.	Records Management.....	7
12.0.	Public Records Exceptions.....	7
13.0.	Definitions .....	7

## Security Planning (PL-1)

### 1.0. Purpose

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

### 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

- 3.1. 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 any 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).
- 4.2. *OIT Information Asset Owners:*
  - 4.2.1. Comply with this Policy & Procedures.
- 4.3. *OIT Information Security:*
  - 4.3.1. Owns, executes, and enforces this Policy & Procedures.

### 5.0. Management Commitment

- 5.1. The State of Maine is committed to following this document.

### 6.0. Coordination Among Agency Entities

- 6.1. OIT assists agencies in the development of required System Security Plans and meeting their Information Security Architecture needs. Additionally, as required by statute, OIT establishes and maintains the minimum Rules of Behavior (RoB) for information system users. Agencies may add additional requirements to the RoB to meet specific agency needs but cannot remove requirements as established by OIT.

---

<sup>1</sup> <https://nvd.nist.gov/800-53/Rev4/control/PL-4>

## Security Planning (PL-1)

### 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. 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 serve as the baseline procedures that are implemented to meet security planning requirements. For information assets under its purview, the Office of Information Technology does the following:
- 8.2. **System Security Plan and Concept of Operations (PL-2):**
  - 8.2.1. OIT Information Security assists the agencies in the development of System Security Plans (SSPs) to meet federal regulatory requirements or as otherwise required.
  - 8.2.2. OIT assists Maine Department of Health and Human Services Office of Family Independence (DHHS-OFI) to develop an SSP and comply with the mandates of the Patient Protection and Affordable Care Act of 2010 ("Affordable Care Act" or "ACA") as determined by the centers for Medicare and Medicaid Services (CMS).
  - 8.2.3. OIT also assists the following agencies that receive Federal Tax Information (FTI) in the preparation of their respective SSPs as determined by the Internal Revenue Services (IRS):
    - 8.2.3.1. DHHS;
    - 8.2.3.2. Maine Department of Labor (DOL), Bureau of Unemployment Compensation; and
    - 8.2.3.3. Maine Department of Administrative and Financial Services (DAFS), Maine Revenue Services (MRS).
  - 8.2.4. 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 annually to the IRS by the May 30<sup>th</sup> due date.
  - 8.2.5. OIT Assists DHHS and DOL with the completion of their 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.

## Security Planning (PL-1)

### 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 and use of State of Maine assets. See the Rules of Behavior for Information Security (PL-4) for more information.

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

8.4.1. OIT, in its [General Architecture Principles](#),<sup>2</sup> 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;

8.4.1.1.1. One (1) of the eight (8) 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;

8.4.1.2.1. 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 one of the top product selection criterion is 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 have to overcome multiple safeguards to achieve their objective.

8.4.3. Security architecture for information systems is consistent with the enterprise [Information Security Policy](#), which establishes the minimum benchmark and implements controls to protect State information assets from

---

<sup>2</sup> <https://www.maine.gov/oit/architecture/documents/GeneralArchitecturePrinciples.pdf>

## Security Planning (PL-1)

unauthorized use, disclosure, modification, and destruction, and to ensure the confidentiality, integrity, and availability of information assets.<sup>3</sup>

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](#),<sup>4</sup> the [Remote Hosting Policy](#),<sup>5</sup> the [User Device and Commodity Application Policy](#),<sup>6</sup> and [Mobile Device Policy](#),<sup>7</sup> 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](#)<sup>8</sup> for more information.

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

8.4.5. IT Vendor Management, 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: 24 June 2020

9.2. Latest Revision Date: 24 June 2020

---

<sup>3</sup> <https://www.maine.gov/oit/policies/SecurityPolicy.pdf>

<sup>4</sup> <https://www.maine.gov/oit/policies/NetworkDeviceManagementPolicy.pdf>

<sup>5</sup> <https://www.maine.gov/oit/policies/RemoteHostingPolicy.pdf>

<sup>6</sup> <https://www.maine.gov/oit/policies/UserDeviceCommodityAppPolicy.pdf>

<sup>7</sup> <https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf>

<sup>8</sup> <https://www.maine.gov/oit/policies/waiver.pdf>

## Security Planning (PL-1)

- 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<sup>9</sup>
- 9.6. Waiver Process: Waiver Policy<sup>10</sup>

### 10.0. Review

- 10.1. 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

- 11.1. 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

- 12.1. 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. *Authorization boundary*: An authorization boundary contains all components of an information system that are authorized for operation and excludes separately authorized systems, to which the information system is connected.
- 13.2. *Federal Taxpayer Information (FTI)*: FTI consists of 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).

Source: [IRS Publication 1075](https://www.irs.gov/pub/irs-pdf/p1075.pdf).<sup>11</sup>

- 13.3. *Information System*: Used interchangeably with *Information Asset*. A discrete, identifiable piece of information technology, including hardware, software,

---

<sup>9</sup> <https://legislature.maine.gov/statutes/5/title5ch163sec0.html>

<sup>10</sup> <https://www.maine.gov/oit/policies/waiver.pdf>

<sup>11</sup> <https://www.irs.gov/pub/irs-pdf/p1075.pdf>

## Security Planning (PL-1)

firmware, systems, services, and related technology assets used to execute work on behalf of OIT or another State agency. (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30).

- 13.4. *Principle of Least Privilege*: A security principle where users are assigned the minimal access necessary to perform their job responsibilities. Access is granted for the shortest duration possible.
- 13.5. *Protected Health Information (PHI)*: PHI means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. It includes information that is protected by the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the “HITECH Act”) and the federal regulations published at 45 C.F.R. parts 160 and 164 (collectively “HIPAA”). This definition excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, in employment records held by a covered entity in its role as employer, and regarding a person who has been deceased for more than 50 years.

Source: [45 CFR § 160.103](#).<sup>12</sup>

- 13.6. *Personally Identifiable Information (PII)*: Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother’s maiden name, etc.). It also includes personal information protected from disclosure under federal or state privacy laws.

Source: [NIST CSRC Glossary](#).<sup>13</sup> Maine state law does not define PII, but rather provides a more limited definition of “personal information” within the context of the Maine Notice of Risk to Personal Data Act (see [10 M.R.S. §1347](#)).<sup>14</sup>

---

<sup>12</sup> <https://www.govinfo.gov/content/pkg/CFR-2017-title45-vol1/pdf/CFR-2017-title45-vol1-sec160-103.pdf>

<sup>13</sup> <https://csrc.nist.gov/glossary>

<sup>14</sup> <http://legislature.maine.gov/legis/statutes/10/title10sec1347.html>