



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

Security Awareness and Training Policy (AT-1)

Table of Contents

1.0 Purpose..... 3
2.0 Scope..... 3
3.0 Conflict..... 3
4.0 Roles and Responsibilities 3
5.0 Management Commitment..... 4
6.0 Coordination Among Agency Entities..... 4
7.0 Compliance..... 4
8.0 Procedures 5
9.0 Document Details..... 7
10.0 Review..... 7
11.0 Records Management..... 7
12.0 Public Records Exceptions..... 7
13.0 Definitions 7
14.0 Abbreviations..... 8

Security Awareness and Training Policy (AT-1)

1.0 Purpose

The purpose of this document is to outline the State of Maine's policy and procedures for security awareness and training. This corresponds to the Awareness and Training (AT) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0 Scope

This document applies to all State of Maine Executive Branch personnel, both employees and contractors.

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 Enforces this policy as outlined in section 7.0, Compliance.

4.1.2 Establishes and conducts privacy training to meet regulatory requirements and business needs.

4.1.3 Ensures that agency personnel have access to and receive the enterprise security awareness training (see Definitions) at required intervals. This includes:

4.1.3.1 Ensuring that agency personnel with access to State email receive the enterprise security awareness training delivered by the Office of Information Technology.

4.1.3.2 Ensuring that agency personnel without access to State email are provided with alternative access to the enterprise security awareness training.

4.1.4 Determines agency personnel security awareness training requirements that extend beyond the enterprise security awareness training.

4.1.5 Ensures agency personnel are aware of all applicable penalties for noncompliance. (See section 7.0).

4.1.6 Maintains agency personnel security awareness training records, in accordance with State of Maine and any additional statutory records retention requirements that apply.

4.1.7 Develops and implements agency-level policy and procedures to meet Federal statutory requirements pertinent to security awareness and training.

4.2 OIT Information Security Office

4.2.1 Owns, executes, and shares responsibility for enforcement of this policy.

4.2.2 Determines the training modules and content to be included in enterprise security awareness training.

4.2.2.1 Delivers enterprise security awareness training to agency personnel who have a State email account.

4.2.2.2 Makes records of training delivered available to authorized agency personnel.

Security Awareness and Training Policy (AT-1)

- 4.2.2.3 Consults with agencies to help determine the training delivery mechanisms and options to meet agency security awareness training requirements that extend beyond the enterprise security awareness training.
- 4.2.2.4 Conducts agency phishing (see Definitions) exercises.

5.0 Management Commitment

The State of Maine is committed to following this document.

6.0 Coordination Among Agency Entities

The Office of Information Technology (OIT) coordinates with agencies to deliver enterprise security awareness training in accordance with [Executive Order 25 FY 20/21](#).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 violations.
- 7.3 Personnel are also subject to penalties for violations of statutory compliance requirements. Depending on the requirement and the nature of the violation penalties could include fines and criminal charges.
 - 7.3.1 Two distinct compliance scenarios
 - 7.3.1.1 Failure to complete the mandated training within the mandated timeframe and
 - 7.3.1.2 Repeatedly failing the simulated phishing tests.
- 7.4 Failure to complete the mandated training within the mandated timeframe results in progressive discipline. This will be decided through collaboration between Agency Management and the Department of Administrative and Financial Services (DAFS) Bureau of Human Resources.
- 7.5 Repeatedly failing the simulated phishing tests results in a combination of additional tiered Security training and progressive discipline. The details of the additional tiered security training will be decided through collaboration between Agency Management and the OIT Information Security Office. The OIT Information Security Office can provide Agency Management with a suggested sample of additional, tiered security training. But, ultimately, it is the responsibility of Agency Management to track and manage the details of the additional tiered security training. Any progressive discipline due to repeated failing of the simulated phishing tests will be decided through collaboration between Agency Management and the DAFS Bureau of Human Resources.

¹ <https://www.maine.gov/governor/mills/sites/maine.gov.governor.mills/files/inline-files/EO%2082%2025.pdf>

Security Awareness and Training Policy (AT-1)

8.0 Procedures

8.1 The following standards apply to the State of Maine's security awareness and training planning capabilities. They represent the base set of procedural requirements.

8.2 Security Awareness Training (AT-2, AT-2(2))

8.2.1 Agencies ensure their personnel receive enterprise security awareness training, which includes content on recognizing, and reporting, potential indicators of insider threat (see Definitions):

8.2.1.1 As part of initial training for new users (onboarding);

8.2.1.2 When required by information system changes; and

8.2.1.3 At least annually thereafter.

8.2.2 State of Maine employee orientation informs new personnel of security awareness training requirements. New employees are informed about their duties regarding confidentiality, privacy, and conflict of interest, as documented in the [Employee Handbook](#).²

8.2.3 The OIT Information Security Office delivers enterprise security awareness training that includes content on recognizing and reporting potential indicators of insider threat to agency users with email addresses by:

8.2.3.1 Querying the Active Directory each month to identify new agency users, so agencies do not need to inform the OIT Information Security Office of new hires.

8.2.3.2 Automatically pushing out enterprise security awareness training to new agency personnel (new Active Directory users).

8.2.3.3 Automatically pushing out enterprise security awareness training to agency personnel annually, thereafter.

8.2.3.4 Delivering enterprise security awareness training to agency personnel at other intervals, upon agency request (such as when required by information system changes).

8.2.3.5 Maintaining a list of agency personnel who have not received enterprise security awareness training.

8.2.3.6 Redelivering training at set intervals, as necessary.

8.2.4 Agencies are responsible for the delivery of enterprise security awareness training for any agency personnel who do not have a State email address.

8.2.5 For each Executive Branch agency, the OIT Information Security Office conducts quarterly phishing exercises that simulate cyberattacks. The schedule is randomized, so agency exercises can occur at any time during a particular quarter.

² <https://www.maine.gov/bhr/sites/maine.gov.bhr/files/inline-files/EmployeeHandbook.pdf>

Security Awareness and Training Policy (AT-1)

8.3 Role-Based Security Training (AT-3)

- 8.3.1 Agencies must determine the appropriate content of security training based on the assigned roles and responsibilities of personnel, regulatory requirements, and the information systems to which personnel have authorized access.
- 8.3.2 Agencies must ensure that personnel with assigned security roles and responsibilities receive role-based security training:
 - 8.3.2.1 Before authorizing access to information, an information system, or performing assigned duties that require access to Personally Identifiable Information (PII) (see Definitions) or other sensitive information;
 - 8.3.2.2 When required by information system changes; and
 - 8.3.2.3 At least annually thereafter.
- 8.3.3 If agency security awareness training requirements extend beyond enterprise security awareness training, then the agency consults with the OIT Information Security Office to help determine the training delivery mechanism and options.
- 8.3.4 The OIT Information Security Office does not currently offer agencies role-based training, which is typically identified and fulfilled through individual professional development plans and through the training, testing, and exercise components of agency contingency or incident response plans.
- 8.3.5 OIT internally completes role-based security training as described in 8.3.4 and in [Contingency Plan Training, Testing and Exercise Procedures \(IR-2, CP-3, IR-3, and CP-4\)](#)³ (intranet only).

8.4 Security Training Records (AT-4)

- 8.4.1 Agencies must retain individual training records in accordance with the [State Archives Records General Retention Schedule](#),⁴ and any other applicable regulatory requirements for records retention.
- 8.4.2 The OIT Information Security Office monitors and maintains security awareness training records for any training it delivers.
- 8.4.3 At the completion of training, personnel are instructed to keep their certificates of completion.
- 8.4.4 The training portal keeps a historical record of agency personnel who complete the training.

³ <http://inet.state.me.us/oit/policies/documents/TrainingTestingExercises.pdf>

⁴ <https://www.maine.gov/sos/arc/records/state/generalschedules.html>

Security Awareness and Training Policy (AT-1)

8.4.5 The OIT Information Security Office makes agency training completion reports available to designated agency personnel, upon request.

9.0 Document Details

9.1 Initial issue Date: March 11, 2014

9.2 Latest Revision Date: June 30, 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](#).⁵

9.6 Waiver Process: [Waiver Policy](#)⁶

9.7 Distribution: [Internet](#)⁷

10.0 Review

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

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 are retained for three years and then destroyed, in accordance with guidance provided by Maine State Archives. Retention of these documents is subject to State Archives General Schedule revisions.

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 Enterprise Security Awareness Training: Training that provides a basic understanding of the need for information security and user actions to maintain security and privacy and to respond to suspected security and privacy incidents. The content also addresses awareness of the need for operations security and privacy related to the organization's information security program.

13.2 Insider Threat: The potential for individuals (e.g., employees, contractors, former employees) to use insider knowledge of sensitive agency information (e.g., security

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

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

⁷ <https://www.maine.gov/oit/policies-standards>

Security Awareness and Training Policy (AT-1)

practices, systems that hold sensitive data) to perform malicious actions, including unauthorized access or disclosure of Personally Identifiable Information or other sensitive information.

- 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](#).⁸
- 13.4 Phishing: The practice of sending fraudulent communications that appear to come from a reliable source, usually through email, with the goal of stealing data, such as credit card or login information, or to install malware on the recipient's machine.
- 13.5 Sensitive Information: Information that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. Sensitive information may include PII, and is protected against unwarranted disclosure, and typically carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse (e.g., Federal tax, protected health, criminal justice, or Social Security information). Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.

14.0 Abbreviations

- 14.1 DAFS: Department of Administrative and Financial Services
- 14.2 FOAA: (Maine) Freedom of Access Act
- 14.3 NIST: National Institute of Standards and Technology
- 14.4 OIT: Office of Information Technology
- 14.5 PII: Personally Identifiable Information

⁸ <https://csrc.nist.gov/glossary>