# Table of Contents

Table of Contents .................................................................................................................................................. 2  
1.0 Document Purpose: ........................................................................................................................................ 3  
2.0 Scope:............................................................................................................................................................... 3  
3.0 Policy 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 History and Distribution: ................................................................................................................ 7  
10.0 Document Review: ......................................................................................................................................... 8  
11.0 Records Management: .................................................................................................................................. 8  
12.0 Public Records Exceptions: ............................................................................................................................ 8  
13.0 Definitions: ....................................................................................................................................................... 8
1.0 **Document Purpose:**

The purpose of this document is to outline the State of Maine’s policy and procedures for security awareness and training.

2.0 **Scope:**

This policy applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

2.1 Executive Branch Agency *information assets*, irrespective of location; and

2.2 Information assets from other State government branches that utilize the State network.

3.0 **Policy Conflict:**

If this policy 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 **Agencies are responsible for:**

4.1.1 Ensuring agency personnel have access to and receive the *enterprise security awareness training*, at required intervals. This includes:

4.1.1.1 Ensuring that agency personnel with access to state e-mail receive the enterprise security awareness training delivered by the Office of Information Technology.

4.1.1.2 Ensuring that agency personnel who do not have access to state e-mail are provided with alternative access to receive enterprise security awareness training.

4.1.2 Determining agency personnel security awareness and training requirements, that extend beyond enterprise security awareness training.

4.1.3 Ensuring agency personnel are aware of all applicable penalties for non-compliance. This includes the penalties identified in Section 7.0 of this policy.

4.1.4 Maintaining agency personnel security awareness training records, in accordance with State of Maine and any additional statutory records retention requirements.
4.1.5 Developing and implementing agency-level policy and procedures, to meet any additional, federal statutory requirements, pertinent to security awareness and training.

4.2 Office of Information Technology:

4.2.1 Chief Information Security Officer (CISO) is responsible for:

4.2.1.1 Owning, executing, and enforcing this policy.

4.2.2 Information Security Office is responsible for:

4.2.2.1 Determining the training modules/content to be included in enterprise security awareness training.

4.2.2.2 Delivering enterprise security awareness training to agency personnel who have a state email account.

4.2.2.3 Making training records available, for training delivered, to authorized agency personnel.

4.2.2.4 Consulting with agencies to help determine the training delivery mechanisms/options to meet agency security awareness training requirements that extend beyond enterprise security awareness training.

4.2.2.5 Conducting agency phishing exercises.

5.0 Management Commitment:

The State of Maine is committed to following this policy and the procedures that support it.

6.0 Coordination Among Agency Entities:

The Office of Information Technology coordinates with agencies to deliver enterprise security awareness training in accordance with Executive Order 2014-003.

7.0 Compliance:

7.1 For State of Maine employees, failure to comply with the procedures identified in this policy may result in progressive discipline up to and including dismissal.

---

1 http://www.maine.gov/tools/whatsnew/attach.php?id=626944&an=1
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 non-State of Maine personnel 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:

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

8.1 Security Awareness Training (AT-2 including CE-2):

8.1.1 Agencies must ensure their personnel receive enterprise security awareness training, which includes content on recognizing and reporting potential indicators of insider threat:

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

8.1.1.2 When required by information system changes;

8.1.1.3 At least annually, thereafter.

8.1.1.3.1 State of Maine employee orientation informs new personnel of security awareness training requirements.

8.1.1.3.2 As part of orientation, new employees are informed about their duties regarding confidentiality, privacy, and conflict of interest, as documented in the Employee Handbook.

8.1.1.3.3 The Information Security Office delivers enterprise security awareness training, that includes content on recognizing and reporting potential indicators of insider threat, to agency users with e-mail addresses by:

8.1.1.3.3.1 Querying Active Directory each month to identify new agency users. This is so agencies do not need to inform the Information Security Office of new hires.

Security Awareness and Training Policy and Procedures (AT-1)

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

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

8.1.1.3.3.4 Delivering enterprise security awareness training to agency personnel at other intervals, upon agency request (e.g., when required by information system changes).

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

8.1.1.3.3.5.1 Re-delivering training, at set intervals, as necessary.

8.1.1.3.4 Agencies are responsible for the delivery of enterprise security awareness training for any agency personnel without a state e-mail address.

8.1.2 The Information Security Office conducts quarterly phishing exercises, that simulate actual cyber attacks, for each executive branch agency.

8.1.2.1 The schedule is randomized, so agency exercises could occur at any time during a particular quarter.

8.2 Role-Based Security Training (AT-3):

8.2.1 Agencies must determine the appropriate content of security and privacy training based on the assigned roles and responsibilities of personnel and the specific security and privacy regulatory requirements and the information systems to which personnel have authorized access.

8.2.2 Agencies must ensure that personnel with assigned security roles and responsibilities receive role-based security training:

8.2.2.1 Before authorizing access to information, an information system or performing assigned duties that require access to Personally Identifiable Information (PII) or other sensitive information;

8.2.2.2 When required by information system changes;

8.2.2.3 At least annually thereafter.
8.2.2.3.1 If agency security awareness training requirements extend beyond enterprise security awareness training, the agency consults with the Information Security Office to help determine the training delivery mechanism / options.

8.2.2.3.2 The Information Security Office does not currently offer role-based training, but a PII module is part of the required enterprise security awareness training.

8.2.2.3.3 Role-based security training is typically identified and fulfilled through individual professional development plans and/or through the training, testing, and exercise components of agency contingency or incident response plans.

8.3 Security Training Records (AT-4):

8.3.1 Agencies must retain individual training records in accordance with the State Archives Records General Retention Schedule\(^3\) and any other applicable regulatory requirements for records retention.

8.3.1.1 The Information Security Office monitors and maintains security awareness training records for any training it delivers.

8.3.1.1.1 At the completion of training, personnel are instructed to keep their certificates of completion.

8.3.1.1.2 The training portal keeps a historical record of agency personnel who complete the training.

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

9.0 Document History and Distribution:

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Log</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>Initial Publication</td>
<td>March 18, 2019</td>
</tr>
</tbody>
</table>

Approved by: Chief Information Security Officer (OIT).

Legal Citation: Title 5, Chapter 163: Office of Information Technology\(^4\).

---

\(^3\) https://www.maine.gov/sos/arc/records/state/generalschedules.html
\(^4\) http://legislature.maine.gov/statutes/5/title5ch163sec0.html
Distribution

This document will be distributed to all appropriate State of Maine personnel and will be posted on the OIT website (https://www.maine.gov/oit/policies).

10.0 Document Review:

This document is to 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 (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, 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: The content includes 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 Information Assets: Business applications, system software, development tools, utilities, hardware, infrastructure, paper records, etc.

13.3 Insider Threat: The potential for individuals (e.g., employees, contractors, former employees) to use insider knowledge of sensitive agency information (e.g., security practices, systems that hold sensitive data) to perform
malicious actions, including unauthorized access or disclosure of Personally
Identifiable Information (PII) or other sensitive information.

13.4 **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.). Source:
NIST CSRC Glossary\(^5\). Maine state law has a more specific definition in 10
M.R.S. §1347\(^6\).

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.

13.6 **Standard:** A collection of specific (technical and/or procedural)
requirements that must be adhered to.

---

\(^5\) [https://csrc.nist.gov/glossary](https://csrc.nist.gov/glossary)
\(^6\) [http://legislature.maine.gov/legis/statutes/10/title10sec1347.html](http://legislature.maine.gov/legis/statutes/10/title10sec1347.html)