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

Program Management Policy and Procedures (PM-1)

Table of Contents

1.0. Purpose

The purpose of this policy is to provide oversight for organization-wide information security programs to help ensure the confidentiality, integrity, and availability of information processed, stored, and transmitted by State of Maine information systems. The Program Management family provides security controls at the organizational level rather than at the information system (see Definitions) level. This corresponds to the Program Management (PM) 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;

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. Complete Federal regulatory reporting requirements as required.

4.1.2. Implement and enforce the standards for the technical, physical, personnel and cyber-physical aspects of information security for their agency.

4.1.3. Are responsible for the Confidentiality, integrity, and availability of entrusted federal and State of Maine data.

4.2. *Chief Information Officer (CIO)*

4.2.1. Enables the vision, goals, funding, and strategic plan for the Executive Branch of Maine State Government through the thorough and diligent administration of technology.

4.2.2. Implements and enforces the standards for the technical, physical, personnel and cyber-physical aspects of information security for OIT.

4.2.3. Allocates the appropriate amount of resources to the information security program.

4.2.4. Is responsible for the confidentiality, integrity, and availability of State of Maine information systems.

4.3. *Chief Information Security Officer (CISO)*

4.3.1. Establishes and maintains the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

[1] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

4.3.2. Establishes and enforces the standards for the technical, physical, personnel and cyber-physical aspects of information security.
4.3.3. Coordinates, develops, implements, and maintains a State of Maine Executive Branch information security program.
4.3.4. Owns, executes, and enforces this Policy.
4.3.5. Informs involved and affected parties in the event of non-compliance with information security policies.

4.4. *The Information Security Office*
4.4.1. Works with CISO to manage and implement the information security program.

4.5. *OIT Information Asset Owners*
4.5.1. Provide reports or access to information technology tools that detail security metrics to the Information Security Office.
4.5.2. Implement and enforce the standards for the technical, physical, personnel and cyber-physical aspects of information security for their respective assets.
4.5.3. Take appropriate action to secure technology as specified in shared intelligence reports.
4.5.4. In collaboration with Agency Business Partners, hold all vendors/partners for externally-hosted information assets accountable to this Policy and Procedures, within the vendor/partner's span-of-control.

4.6. *IT Procurement*
4.6.1. With support from OIT Information Asset Owners, ensures vendor contracts contain appropriate security requirement and risk management language.

4.7. *The Architecture and Policy Team*
4.7.1. In collaboration with the Information Security Office, develops and maintains Plans of Actions and Milestones (POA&Ms).
4.7.2. In collaboration with the Information Security Office, develops and maintains policy and procedures that detail the security controls required of the security program.

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 program management with agencies to ensure the security of State of Maine information assets in accordance with Executive Order 2014-003[2] and Title 5, Chapter 163 §1971-1985.[3] Agencies and the Office of Information Technology coordinate to meet all state and Federal

[2] http://www.maine.gov/tools/whatsnew/attach.php?id=626944&an=1
[3] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

audit documentation and reporting compliance requirements. Roles and responsibilities in this document establish further coordination of the technical, physical, personnel and cyber-physical aspects of information security.

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 procedures are designed to satisfy the security control requirements of this Policy (Program Management) as outlined in NIST Special Publication 800-53 (Rev. 4),[4] Internal Revenue Service Publication 1075,[5] Centers for Medicare & Medicaid Services Minimum Acceptable Risk Standards for Exchanges 2.0,[6] Criminal Justice Information Services Security Policy,[7] Health Insurance Portability and Accountability Act Security Rule,[8] and to satisfy Federal law.

8.2. Chief Information Security Officer (PM-2)

8.2.1. The CIO designates a CISO who has the explicit authority, mission, and resources to coordinate, develop, implement, and maintain an organization-wide information security program and requirements for the Executive Branch of Maine State government.

8.2.2. The CIO ensures the CISO:

8.2.2.1. Possesses training and experience required to administer the CISO function;

8.2.2.2. Has authority for information security for the Executive Branch of Maine State government; and

8.2.2.3. Has information security duties as the primary job function.

8.2.3. The CISO:

8.2.3.1. Establishes and reviews annually the information security strategy (i.e., program plan) for the Executive Branch of the State of Maine.

8.2.3.2. Develops and maintains information security policies and procedures that address known and potential security risks;

[4] https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
[5] https://www.irs.gov/pub/irs-pdf/p1075.pdf
[6] https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/#MinimumAcceptableRiskStandards
[7] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center
[8] https://www.hhs.gov/hipaa/for-professionals/security/index.html

8.2.3.3. Works with customers and technical resources to ensure that controls to address information security risks are utilized; and

8.2.3.4. Provides guidance to Executive Branch officials, *information system* owners, information custodians, and information users concerning their responsibilities.

8.3. Information Security Resources (PM-3)

8.3.1. OIT conducts information technology security planning in conjunction with the biennial budget process. The Information Security Office formulates its budget request by calculating the number of resources and security services it provides to the agencies.

8.3.1.1. The services are consumed through internal service rates by the agencies.

8.3.1.2. Once approved by the CIO, the budget request is sent to the Department of Administrative and Financial Services for evaluation and approval. The State budget is the shared responsibility of the Legislature and the Governor.

8.3.2. Significant security purchases comply with the justification and documentation requirements set forth by the Division of Procurement Services within the Department of Administrative and Financial Services.

8.3.3. The CISO ensures that security resources are available for expenditure as planned.

8.4. Plan of Action and Milestone Process (PM-4)

8.4.1. POA&Ms for the security program are developed and maintained by the Information Security Office and Architecture and Policy team. POA&Ms associated with organizational information systems that contain actions and milestones necessary to meet compliance and security requirements are developed and maintained by their respective agencies with support from the Information Security Office (see Security Assessment and Authorization Policy and Procedures (CA-1)).[9]

8.4.1.1. The POA&Ms are developed and maintained to document actions, priorities, objectives, tasks, resources, success criteria, and responsibilities to adequately respond to risks to State of Maine operations and assets, individuals, and other organizations.

8.4.1.2. State agencies administering select Federal programs report POA&Ms in accordance with the Federal Information Security Modernization Act[10] reporting requirements; and

[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf

[10] https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

8.4.1.3. The CISO reviews and approves POA&Ms for consistency with the Information Security Office risk management strategy and priorities for risk response actions.

8.4.1.4. Updates to the POA&Ms are based on findings from security control assessments, audits, and continuous monitoring activities.

8.5. Information System Inventory (PM-5)

8.5.1. OIT Enterprise Data Services maintains an inventory of information systems (see Configuration Management Policy and Procedures (CM-8)).[11]

8.6. Information Security Measures of Performance (PM-6)

8.6.1. The CISO develops, monitors, and reports on the results of information security measures of performance through:

8.6.1.1. Dashboards provided by security tools used by the Information Security Office and other Information Asset Owners;

8.6.1.2. Metric reporting of audits outlined in Security Assessment and Authorization Policy and Procedures (CA-1);[12]

8.6.1.3. Metrics provided by third party reports (e.g., Multi-State Information Sharing and Analysis Center);

8.6.1.4. Self-assessment results as a part of the Nationwide Cybersecurity Review (NCSR);

8.6.1.5. Comparative analysis results from surveys submitted by the Information Security Office (e.g., Nationwide Cybersecurity Review, Deloitte-NASCIO Cybersecurity Study Survey 2020) or OIT (e.g., Digital States Survey); and

8.6.1.6. Ad hoc reports as requested by the CISO of the Information Security Office.

8.7. Enterprise Architecture (PM-7, related to PL-8)

8.7.1. OIT, in its General Architecture Principles,[13] outlines guidance to aid in everyday decision-making that:

8.7.1.1. Describes the overall philosophy, requirements, and approach to be taken with regards to protecting the confidentiality, integrity, and availability of information;

8.7.1.1.1. 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.

8.7.1.2. Describes how the information security architecture is integrated into and supports the enterprise architecture;

[11] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/configuration-management-policy.pdf
[12] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf
[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/general-architecture-principles_1.pdf

8.7.1.2.1. OIT describes security in the General Architecture Principles as foundational. Additionally, security is core to the mission of OIT.

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

8.7.1.3.1. 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.

8.7.1.3.2. 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 criteria is cybersecurity, privacy, and accessibility.

8.7.2. 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.

8.7.2.1. Security architecture for information systems is consistent with the enterprise information security plans, policies, and procedures found here[14] with select security control families on the intranet. These documents 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.

8.7.2.2. OIT adopts a NIST security control framework, with which the security architecture of information systems is compliant.

8.7.2.1. Other policies, including but not limited to the Network Device Management Policy,[15] the Remote Hosting Policy,[16] the User Device and Commodity Application Policy,[17] the OIT Application Deployment Certification Policy,[18] the OIT Infrastructure Deployment Certification Policy,[19] and the Mobile Device Policy,[20] ensure the security of State information assets. All public OIT policies can be found at https://www.maine.gov/oit/policies-standards/.

[14] https://www.maine.gov/oit/policies-standards
[15] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/network-device-management-policy.pdf
[16] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/remote-hosting-policy.pdf
[17] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/user-device-commodity-app-policy.pdf
[18] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf
[19] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/infrastructure-deployment-certification.pdf
[20] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/mobile-device-policy.pdf

8.7.2.2. Any information system which is not compliant with OIT policies must go through a rigorous waiver process, which is managed by the Architecture and Policy Team and the Information Security Office and includes 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[21] for more information.

8.7.3. The Architecture and Policy Team, in collaboration with the Information Security Office, the OIT Compliance Officer, IT Procurement, and other relevant parties, coordinates a review of and vets all proposed new technologies and technology solutions presented by OIT or Agency Business Partners to ensure that new products and technologies align with the State of Maine's overall security architecture.

8.7.4. IT Procurement, in collaboration with the Architecture and Policy Team, the Information Security Office, the OIT Compliance Officer, 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.

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

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

8.8. Critical Infrastructure Plan (PM-8)

8.8.1. Homeland Security Presidential Directive 7[22] establishes a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The Maine Emergency Management Agency (MEMA) is the lead agency to coordinate State of Maine efforts in support of the Critical Infrastructure Protection Program.[23]

8.8.2. The Maine Information Analysis Center (MIAC)[24] also plays a role in critical infrastructure planning. A program of the Maine Department of Public Safety, the MIAC is Maine's designated fusion center (see Definitions). The MIAC's mission is to collect, analyze, and appropriately share intelligence between the Federal government and the State of Maine.

[21] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[22] https://www.cisa.gov/homeland-security-presidential-directive-7
[23] https://www.maine.gov/mema/homeland-security/critical-infrastructure-protection
[24] https://www.maine.gov/dps/msp/specialty-units/MIAC

8.8.3. The CISO supports the protection of Critical Infrastructure Planning by:
- 8.8.3.1. Supporting MEMA planning efforts (e.g., Comprehensive Emergency Management Plan);
- 8.8.3.2. Maintaining a formalized relationship with the MIAC (i.e., Memorandum of Understanding) to increase collaboration, information sharing, and support for Federal, State, and county stakeholders; and
- 8.8.3.3. Performing its day-to-day information security mission to include the development contingency plans related to improving business resiliency.

8.9. Risk Management Strategy (PM-9)

8.9.1. For OIT-hosted information assets:
- 8.9.1.1. OIT works with agencies to classify data based on risk, so that data may be used and protected appropriately. OIT has adopted the Traffic Light Protocol (see Definitions) described in the Data Classification Policy[25] for this purpose.
- 8.9.1.2. As part of the risk management strategy, risk is managed throughout the system development lifecycle in accordance with the following policies:
  - 8.9.1.2.1. OIT Application Deployment Certification Policy[26]
  - 8.9.1.2.2. OIT Application Deployment Certification Handbook[27]
  - 8.9.1.2.3. OIT Infrastructure Deployment Certification Policy[28]
  - 8.9.1.2.4. OIT Software Development Lifecycle Procedure[29]
  - 8.9.1.2.5. OIT Software Development Lifecycle Policy[30]
- 8.9.1.3. OIT manages risk to information assets by proactively scanning and addressing discovered vulnerabilities in a timely fashion, in accordance with the Vulnerability Scanning Procedure (RA-5).[31]
- 8.9.1.4. Risk assessment is carried out in accordance with the OIT Risk Assessment Policy and Procedure (RA-1).[32]
- 8.9.1.5. Based on the data that resides on OIT systems, and the regulatory regime they are subjected to, risk levels are routinely audited by external partners (usually Federal regulatory agencies) (see OIT

[25] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[26] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf
[27] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification-guidelines_1.pdf
[28]https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/infrastructure-deployment-certification.pdf
[29] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-procedure.pdf
[30] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-policy.pdf
[31] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/vulnerablity-scanning-procedure.pdf
[32] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/risk-assessment-policy-procedure.pdf

Security Assessment and Authorization Policy and Procedures (CA-1)).[33]

8.9.1.6. OIT also hires third party vendors to conduct independent risk assessments. These vendors are required to produce reports including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the in-scope information system, and the information it processes, stores, or transmits. These reports are maintained by the OIT Information Security Office. OIT shares risk assessment results to affected stakeholders on a need-to-know basis.

8.9.1.7. OIT reviews and updates the risk management strategy and all applicable risk management policies on an annual basis or as required to address organizational changes.

8.9.2. For remote-hosted information assets, the Hosting Partner is responsible for risk management, with oversight from OIT Application Development Teams in collaboration with IT Procurement and Agency Business Partners, in accordance with the Remote Hosting Policy.[34]

8.10. **Security Authorization Process (PM-10)**

8.10.1. The CIO is the senior-level executive, head of OIT, who serves as the authorizing official for applications and computer infrastructure for State of Maine agencies. The CIO and the CISO delegate as they see fit to other participants of the Information Security Office.

8.10.2. OIT works with agencies to complete security assessments to fulfill Federal regulatory requirements or as otherwise required in accordance with the Security Assessment and Authorization Policy and Procedures (CA-1).[35]

8.10.3. Security authorization (see Definitions) occurs as part of deployment certification and as part of change management (see Change Management Policy and Procedures).[36]

8.10.3.1. OIT manages, documents, tracks, and reports on the security state of information systems and the environments in which those systems operate through security authorization processes.

8.10.4. Prior to deployment, infrastructure, systems, and applications are subject to the following policies and procedures:

[33] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf
[34] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/remote-hosting-policy.pdf
[35] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf
[36] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

8.10.4.1. OIT Application Deployment Certification Policy[37]
8.10.4.2. OIT Application Deployment Certification Handbook[38]
8.10.4.3. OIT Infrastructure Deployment Certification Policy[39]
8.10.4.4. OIT Software Development Lifecycle Procedure[40]
8.10.4.5. OIT Software Development Lifecycle Policy[41]

8.10.5. Routine scans of information assets are carried out in accordance with the Vulnerability Scanning Procedure (RA-5).[42]

8.10.6. Continuous monitoring of information assets is carried out in accordance with the Security Assessment and Authorization Policy and Procedures (CA-1).[43]

8.10.7. Results of security assessments as well as deployment certification tests, Software Development Lifecycle tests, and routine scans are documented in the Enterprise Ticketing System or Jira.

8.10.8. The security assessment and authorization process is part of the organizational risk management program.

8.11. Mission/Business Process Definition (PM-11)

8.11.1. As defined by statute, the mission of the Office of Information Technology includes providing high-quality, responsive, cost-effective information technology services to the agencies, instrumentalities, and political subdivisions of State Government. Additionally, the CIO is responsible for setting security standards for the use of information and telecommunications technologies, and the CIO and OIT are responsible for the protection of data files (Title 5, Chapter 163: Office of Information Technology).[44] Therefore, OIT has established the Information Security Office and made security foundational to everything else to protect State and citizen data (see General Architecture Principles).[45]

---

[37] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf
[38] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification-guidelines_1.pdf
[39]https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/infrastructure-deployment-certification.pdf
[40] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-procedure.pdf
[41] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/sdlc-policy.pdf
[42] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/vulnerablity-scanning-procedure.pdf
[43] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf
[44] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[45] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/general-architecture-principles_1.pdf

8.11.2. Additionally, OIT is subject to Federal audits, and part of OIT's business process is to meet these Federal audit requirements, which also ensures strong security and privacy for State and citizen data.

8.11.3. The Information Security Office works with agencies and subject matter experts to implement appropriate measures for information protection (see OIT Risk Assessment Policy and Procedure (RA-1).[46]

8.12. **Insider Threat Program (PM-12)**

8.12.1. The insider threat (see Definitions) program includes:

8.12.1.1. Conducting select background checks for personnel for review by the Bureau of Human Resources.

8.12.1.2. Administering required insider threat security awareness training as part of initial training for new users, when required by information system changes, and at least annually, in accordance with the Security Awareness Training Policy (AT-1).[47]

8.12.1.3. Implementing security controls to prevent malicious insider user activity, including:

8.12.1.3.1. Employing the principle of least privilege (see Access Control Procedures for Users);[48]

8.12.1.3.2. Generating audit records, reviewing audit records for indications of malicious insider activity, employing non-repudiation mechanisms, and monitoring for evidence of unauthorized disclosure of State information (see Audit and Accountability Policy and Procedures, coming soon);

8.12.1.3.3. Employing continuous monitoring for information systems (see Security Assessment and Authorization Policy and Procedures (CA-5));[49]

8.12.1.3.4. Managing information system identifiers (see Identification and Authentication Policy and Procedures (IA-1),[50] intranet only);

8.12.1.3.5. Prohibiting the use of personally owned, non-State controlled media and devices with State information assets (see Rules of Behavior);[51]

8.12.1.3.6. Issuing physical access authorization only to authorized individuals (see Physical and Environmental Security Policy and Procedures, upon publication);

---

[46] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/risk-assessment-policy-procedure.pdf
[47] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-awareness-training-policy.pdf
[48] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/access-control-procedures-for-users.pdf
[49] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf
[50] http://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf
[51] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf

8.12.1.3.7. Revoking authenticators/credentials, disabling information system access, and retrieving security-related information system-related property for terminated personnel, and, as needed, transferred personnel (see Personnel Security Policy and Procedures, coming soon);

8.12.1.3.8. Implementing boundary protection and operations security; and

8.12.1.3.9. Monitoring information systems to detect unauthorized use and connections (see System and Information Integrity Policy and Procedures (SI-1)).[52]

8.12.1.4. Conducting threat response and mitigation including insider threats, detailed in the Cyber Incident Response Plan (IR-8)[53] (intranet only) and the Cyber Incident Response Policy and Procedures (IR-1)[54] (intranet only).

8.13. Information Security Workforce (PM-13)

8.13.1. The OIT information security workforce operates under the direction and supervision of the CISO.

8.13.2. The knowledge and skill levels to perform information security duties and tasks are outlined in the job description and requirements of positions with information security duties and tasks.

8.13.3. Individual development plans for personnel with information security duties and tasks are developed in collaboration between the employee and manager during the annual performance review process. These also ensure that personnel obtain and maintain certification and training on an ongoing basis.

8.13.4. The annual performance review process ensures information security workforce personnel obtain and continue to meet individual qualification standards for their assigned information security roles.

8.13.5. OIT offers a training stipend for certain job classifications, tuition reimbursement for relevant courses, certificates, degree programs, and employee access to online learning platforms in order to encourage growth and develop a strong information security workforce.

8.13.6. As risks, threats, and the organization itself changes, workforce knowledge and skills are re-evaluated and remediated using the above-mentioned employee development tools.

[52] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/system-information-integrity-policy.pdf
[53] http://inet.state.me.us/oit/policies/documents/IncidentResponsePlan.pdf
[54] http://inet.state.me.us/oit/policies/documents/IncidentResponsePolicy.pdf

8.13.7. Security awareness training is required for all employees at least annually (see Security Awareness Training Policy (AT-1)).[55] Role-based security awareness training is administered within OIT in accordance with Contingency Plan Training, Testing, and Exercise Procedures (intranet only).[56]

8.14. **Testing, Training, and Monitoring (PM-14)**

8.14.1. The procedures for security testing are detailed in Security Assessment and Authorization Policy and Procedures (CA-1);[57]

8.14.1.1. This policy is reviewed and updated as required, and at least annually, to reflect an evolving information security environment and to ensure consistency with the organizational risk management strategy and priorities for risk response actions.

8.14.1.2. The Information Security Office, in collaboration with Agency Business Partners and other units within OIT, ensures that testing procedures are executed in a timely manner.

8.14.1.3. Information assets undergo routine scans.

8.14.2. The procedures for testing contingency plans and incident response plans are detailed in Contingency Plan Training, Testing, and Exercise Procedures (intranet only).[58]

8.14.2.1. This policy is reviewed and updated as required, and at least annually, to reflect an evolving information security environment and to ensure consistency with the organizational risk management strategy and priorities for risk response actions.

8.14.2.2. The Information Security Office ensures that testing procedures are executed in a timely manner.

8.14.2.2.1. Exercises to test security incident response capabilities are conducted periodically, and at least annually.

8.14.3. The procedures for security training are detailed in the Security Awareness Training Policy (AT-1).[59] The plan for contingency plan training is detailed in Contingency Plan Training, Testing, and Exercise Procedures (intranet only).[60]

8.14.3.1. These policies are reviewed and updated as required, and at least annually, to reflect an evolving information security environment and to ensure consistency with the organizational risk management strategy and priorities for risk response actions.

---

[55] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-awareness-training-policy.pdf
[56] http://inet.state.me.us/oit/policies/documents/TrainingTestingExercises.pdf
[57] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf
[58] http://inet.state.me.us/oit/policies/documents/TrainingTestingExercises.pdf
[59] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-awareness-training-policy.pdf
[60] http://inet.state.me.us/oit/policies/documents/TrainingTestingExercises.pdf

8.14.3.2. The Information Security Office and Agency Business Partners share the responsibility for ensuring training plans are executed in a timely manner.

8.14.4. The procedures for information system monitoring are detailed in System and Information Integrity Policy and Procedures (SI-1).[61] The plan for continuous monitoring is detailed in Security Assessment and Authorization Policy and Procedures (CA-1);[62]

8.14.4.1. These policies are reviewed and updated as required, and at least annually, to reflect an evolving information security environment and to ensure consistency with the organizational risk management strategy and priorities for risk response actions.

8.14.4.2. The Information Security Office is responsible for ensuring these monitoring procedures are executed in a timely manner.

8.15. Contacts with Security Groups and Associations (PM-15)

8.15.1. The Office of Information Technology has established institutional contacts with Federal, State, and private companies within the security community. These entities OIT contacts routinely are the same entities OIT contacts as a part of cyber incident response procedures detailed in the Cyber Incident Response Plan (IR-8)[63] (intranet only).

8.15.2. Conferences, research, publications, and information exchanges provided by institutional contacts facilitates ongoing security education and training for Information Security Office personnel.

8.16. Threat Awareness Program (PM-16)

8.16.1. The Office of Information Technology's threat awareness program includes cross-organizational information sharing with organizations as described in 8.15.1.

8.16.2. Information shared with the Information Security Office is further shared with the impacted Information Asset Owners and Agency Business Partners for action as required.

8.16.3. Annual security awareness training as part of initial training for new users, when required by information system changes, and at least annually is another component of the Threat Awareness Program.

8.16.4. The Information Security Office routinely conducts phishing exercises to maintain employee vigilance on threats.

---

[61] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/system-information-integrity-policy.pdf
[62] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-assessment-authorization-policy.pdf
[63] http://inet.state.me.us/oit/policies/documents/IncidentResponsePlan.pdf

8.16.5. The Information Security Office provides additional threat awareness training to Agency Business Partners through its support of National Cyber Security Awareness Month in October and as required.

9.0. Document Details

9.1. Initial Issue Date: June 30, 2021
9.2. Latest Revision Date: November 03, 2023
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[64]
9.6. Waiver Process: Waiver Policy[65]
9.7. Distribution: Internet[66]

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, 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. Information System: Used interchangeably with information asset. A discrete, identifiable piece of information technology, including hardware, software, firmware, systems, services, and related technology assets used to execute work on behalf of OIT or another State agency.

[64] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[65] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[66] https://www.maine.gov/oit/policies-standards

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

13.3. Fusion Center: Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between State, Local, Tribal and Territorial, Federal and private sector partners.
Source: the Department of Homeland Security.[67]

13.4. 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.[68]

13.5. Security Authorization: The official management decision given by a senior official to authorize operation of a system or the common controls inherited by designated organization systems and to explicitly accept the risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Also known as authorization to operate.

13.6. Traffic Light Protocol (TLP): The Cybersecurity and Infrastructure Security Agency (CISA) Traffic Light Protocol (TLP) used by OIT for the classification of PII impact level. OIT's four data, communication, or network classification levels are Public (TLP: White), Internal (TLP: Green), Sensitive (TLP: Amber), and Restricted (TLP: Red) (See Data Classification Policy).[69]

14.0. Abbreviations

14.1. CIO: Chief Information Officer
14.2. CISO: Chief Information Security Officer
14.3. *FISMA:* The Federal Information Security Management Act.[70]
14.4. MEMA: Maine Emergency Management Agency
14.5. MIAC: Maine Information Analysis Center
14.6. NCSR: Nationwide Cybersecurity Review

[67] https://www.dhs.gov/fusion-centers
[68] https://csrc.nist.gov/glossary/term/personally_identifiable_information
[69] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[70] https://www.congress.gov/bill/113th-congress/senate-bill/2521

14.7. NIST: National Institute of Standards and Technology
14.8. OIT: Office of Information Technology
14.9. PII: Personally Identifiable Information
14.10. POA&M: Plan of Actions and Milestones
14.11. TLP: Traffic Light Protocol