Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Information Security Policy

1.0 Purpose

This policy is used as a reference document, with pointers to specific State of Maine policies (National Institute of Standards and Technology (NIST) and otherwise), which establish our *minimum* benchmarks to protect the security of State Information Assets.

2.0 Definitions

2.1 *Agency Data Custodian:* Agency official, who, based on their position, is fiduciary owner of specific Agency Information Assets. For instance, the Labor Bureau of Unemployment Compensation Director (or designee) is the Agency Data Custodian for Unemployment Compensation Information Assets, and the Health & Human Services Office of Family Independence Director (or designee) is the Agency Data Custodian for Benefits Information Assets.

2.2 *Information Assets:* Business applications, system software, development tools, utilities, hardware, infrastructure, storage media, paper records, etc.

2.3 *Privileged User:* The user granted the rights that go beyond that of a typical business user to manage and maintain IT systems. Usually, such rights include administrative access to networks and/or devices. This does not include users with administrative access to their own workstation.

2.4 *Rules of Behavior:* Behavioral standards to facilitate information security, especially relevant to Privileged Users.

3.0 Applicability

This Policy applies to all Information Assets under the purview of the Chief Information Officer (CIO), irrespective of where the Information Assets are hosted.

4.0 Responsibilities

4.1 The Chief Information Officer (or designee) executes this Policy for all Information Assets.

4.2 The Chief Information Security Officer (CISO) (or designee) owns, interprets, and enforces this Policy.

4.3 The Agency Data Custodian (or designee) executes this Policy for all Information Assets under their purview.

5.0 Directives

5.1 **Access Authorization**: Access authorization to any State Information Asset is identified in the Access Control Policy (AC-1).[1]

5.2 **Access Control**: User access control to any State Information Asset is identified in the Access Control Policy (AC-1).[2]

5.3 **Access – Non-State Entities**: Non-State user access control to any State Information Asset is identified in the Access Control Policy (AC-1).[3]

5.4 **Access Rights Review**: Review for access rights of any State Information Asset is identified in the Access Control Policy (AC-1).[4]

5.5 **Background Checks**: Background check requirements are identified in the Personnel Security Policy and Procedure (PS-1).[5]

5.6 **Backups**: Policy regarding backups of any State Information Asset is identified in Backup and Recovery Procedures[6] (Internal only).

5.7 **Data Classification**: Policy regarding data classification of any State Information Asset is identified in the Data Classification Policy.[7]

5.8 **Documentation**: Documentation for audit and security policy requirements for any State Information Asset is identified in the Audit and Accountability Policy and Procedures (AU)[8] (Internal only).

5.9 **Education & Training**: Information security education and training directives are identified in the Security and Awareness Training Policy and Procedures (AT-1).[9]

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf
[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf
[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf
[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf
[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/PersonnelSecurityPolicy.pdf
[6] https://stateofmaine.sharepoint.com/sites/MaineIT/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies%2FBackupRecoveryProcedures%2Epdf&parent=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies
[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[8] https://stateofmaine.sharepoint.com/sites/MaineIT/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies%2FAuditAccountabilityPolicyProcedures%2Epdf&parent=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies
[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/security-awareness-training-policy.pdf

5.10 **Incident Reporting**: Policy regarding incident reporting is identified in the Cyber Incident Response Policy and Procedures (IR-1)[10] (Internal only) and the Cyber Incident Response Plan (IR-8)[11] (Internal only).

5.11 **Information Asset Maintenance**: Maintenance of any State Information Asset is identified in the Maintenance Policy and Procedures (MA-1)[12] (Internal only).

5.12 **Interconnection Security Agreements**: Policy regarding data exchange that includes any State Information Asset is identified in the Data Exchange Policy.[13]

5.13 **Malwares**: Malware protection for State Information Assets is identified in Configuration Management Policy (CM-1).[14]

5.14 **Passwords**: Password rules are identified in Identification and Authentication Policy and Procedures (IA-1)[15] (Internal only).

5.15 **Physical Protection**: Policy regarding the physical and environmental protection of State Information Assets is identified in Physical and Environmental Protection (PE-1).[16]

5.16 **Devices:** Policy regarding acceptable device use is identified in User Device and Commodity Application Policy[17] and the Network Device Management Policy.[18]

5.17 **Remote, Mobile, and Wireless Access (Safeguarding Portable and Mobile Devices)**: Policy regarding remote and wireless access is identified in Access Control Policy (AC-1).[19] The Mobile Device Policy[20] outlines policy for any mobile device connecting to any State Information Asset.

---

[10] https://stateofmaine.sharepoint.com/sites/MaineIT/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies%2FIncidentResponsePolicy%2Epdf&parent=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies

[11] https://stateofmaine.sharepoint.com/sites/MaineIT/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies%2FIncidentResponsePlan%2Epdf&parent=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies

[12] https://stateofmaine.sharepoint.com/sites/MaineIT/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies%2FMaintenancePolicyProcedures%2Epdf&parent=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies

[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf

[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ConfigurationManagementPolicy.pdf

[15] https://stateofmaine.sharepoint.com/sites/MaineIT/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies%2FIdentificationAuthenticationPolicy%2Epdf&parent=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies

[16] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/PhysicalandEnvironmentalProtection.pdf

[17] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/UserDeviceCommodityAppPolicy.pdf

[18] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/NetworkDeviceManagementPolicy.pdf

[19] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf

[20] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/MobileDevicePolicy.pdf

5.18 **Risk Assessments**: State Information Assets will be assessed for security risks based on the policy outlined in the Risk Assessment Policy and Procedure (RA-1).[21]

5.19 ***Rules of Behavior* for All Users**: Rules of behavior for all users are identified in Rules of Behavior (PL-4).[22]

5.20 **Rules of Behavior for *Privileged Users***: Rules of behavior for privileged users are identified in Rules of Behavior (PL-4).[23]

5.21 **Session Timeout**: Session timeout length is identified in 8.6.2. of the Access Control Policy (AC-1).[24]

5.22 **Static Storage (Data at Rest)**: Data at Rest is identified in 4.9 of System and Communications Protection Procedures for Defense in Depth.[25]

5.23 **Storage Media Disposal**: Media disposal is identified in Media Protection Policy and Procedures (MP-1)[26] (Internal only).

5.24 **Transport Security (Data in Flight)**: Encryption levels for data in flight is identified in the Data Exchange Policy.[27]

5.25 **Unknown Custody Device**: Responsibilities and expected behaviors for anyone using State of Maine information or information assets are identified in Rules of Behavior (PL-4).[28] This policy contains general rules, along with references to other policies containing more in depth guidance for unknown custody devices.

5.26 **Vulnerability Management:** Policy regarding management of vulnerabilities in networks, devices, and applications of State Information Assets is identified in the Vulnerability Scanning Procedure (RA-5).[29]

6.0 Document Details

6.1 Initial Issue Date: May 1, 2012
6.2 Latest Revision Date: May 1, 2024.
6.3 Point of Contact: PolicyTeam.OIT@Maine.Gov
6.4 Approved By: Chief Information Officer, OIT.
6.5 Legal Citation: Title 5, Chapter 163: Office of Information Technology.[30]

---

[21] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RiskAssessmentPolicyProcedure.pdf
[22] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf
[23] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf
[24] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf
[25] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SCDefenseInDepthProcedures.pdf
[26] https://stateofmaine.sharepoint.com/sites/MaineIT/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies%2FMediaProtectionPolicy%2Epdf&parent=%2Fsites%2FMaineIT%2FShared%20Documents%2FPolicies
[27] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf
[28] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RulesofBehavior.pdf
[29] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/VulnerablityScanningProcedure.pdf
[30] http://legislature.maine.gov/statutes/5/title5ch163sec0.html

6.6 Waiver Process: See the Waiver Policy.[31]

[31] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf