State of Maine

Department of Administrative and Financial Services

Office of Information Technology

Access Control Policies and Procedures (AC)

Table of Contents

1.0. Document Purpose

The purpose of this document is to define the State of Maine policy and procedures that are in place for providing access to State of Maine information assets (see Definitions). This part of the security program is focused on protecting the confidentiality (see Definitions), integrity (see Definitions), and availability (see Definitions) of State information assets. This document corresponds to the Access Control (AC) Control Family of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 5).[1]

2.0. Scope

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

2.1.1. Executive Branch Agency information assets, irrespective of location; and

2.1.2. Information assets from other State government branches that use Executive Branch-managed services.

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:

4.1.1. Ensure that any contracts for vendor-hosted or managed agency information assets adhere to any pertinent Federal regulations, State regulations, and Office of Information Technology (OIT) policies, procedures, and standards.

4.1.2. Develop and implement agency-level policy and procedures to meet additional Federal statutory requirements pertinent to agency information asset access controls.

4.1.3. Ensure that the access of any authorized user (see Definitions) to agency information assets is based on the principle of least privilege (see Definitions) and separation of duties (see Definitions).

4.1.4. Assign an agency data custodian (see Definitions) for agency information assets.

4.1.5. Develop and maintain security plans for agency information assets.

[1] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

4.1.6. Approve/deny the initial Long-Term Out-of-State Domestic Remote Access (see Definitions) or Foreign Remote Access (see Definitions) request from Agency personnel; Initiate related ticket workflow in the Enterprise Ticketing System; and

4.1.7. Ensure that agency personnel adhere to all related procedures.

4.2. Chief Information Security Officer (CISO):

4.2.1. Owns, executes, and enforces this Policy and Procedures;

4.2.2. Makes the determination of the risk for a specific Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access request;

4.2.3. Makes the determination of compensating security controls for a specific Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access request;

4.2.4. Informs third party vendors performing continuous monitoring of any resulting exception; and

4.2.5. Depending upon the assessed risk for a specific Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access request, either approves or denies the specific request. If a request is denied, the Chief Information Officer is consulted for a final determination.

4.3. Chief Data Officer (CDO)

4.3.1. Provides enterprise data governance and oversight to ensure that agencies classify, label, and manage data consistently across the State of Maine's environment.

4.3.2. Ensures the implementation of the State's data classification framework and collaborates with agencies to promote consistent application of data labeling, handling, and protection requirements.

4.4. Department of Administrative and Financial Services Bureau of Human Resources:

4.4.1. Completes the initial review for all State employees requesting any out-of-state remote access, regardless of destination (domestic or foreign) or duration (short-term or long-term).

4.5. OIT Leadership:

4.5.1. Assigns an owner for each information asset supported by OIT.

4.6. OIT Information Asset Owners:

4.6.1. Ensure that authorized personnel's access to assigned assets is based on the principle of least privilege;

4.6.2. In collaboration with IT procurement and agencies, hold contracted other parties that host State information assets accountable to this Policy and Procedures; and

4.6.3. Make necessary configuration changes (such as port access, country exceptions, folder access, etc.) for approved Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access requests.

4.7. DAFS IT Procurement:

4.7.1. Collaborates with Information Asset Owners and agencies, hold contracted other parties that host State information assets accountable to this Policy and Procedures.

5.0. Management Commitment

The State of Maine is committed to following this policy and the supporting procedures.

6.0. Coordination Among Agency Entities

6.1. OIT coordinates with agencies to implement and maintain security controls that safeguard agency information assets from unauthorized access by individuals or devices. Active Directory (AD) accounts are established through either the Enterprise Ticketing System or an automated process within the current Human Resources Management System (HRMS).

6.2. Agencies work with their OIT application development managers, account managers, and the OIT Information Security Office to determine how access is managed and who, and under what circumstances, may access agency information assets.

6.3. Application development managers serve as owners for the agency application systems that their teams support. Requests for application access for support go through the application development managers.

6.4. Access to particular parts of the network for administrative work is approved by the information asset owners.

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 the 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

The following standards apply to and represent the security controls established to meet an acceptable level of protection for, State of Maine from unauthorized information system access.

8.1. **Governance Controls: Policy and Procedures (AC-1)** – The OIT develops, approves, disseminates, and reviews this policy in accordance with Sections 9.0 (Document Details) and 10.0 (Review). These sections collectively satisfy NIST SP 800-53 Revision 5 control one (1) requirements for defining, approving, disseminating, and periodically reviewing policy and procedures for this control family.

8.2. **Access Control Procedures for Users (AC-2, AC-3, AC-5, AC-6, AC-17, AC-18, AC-19) -** User access control procedures are identified separately in Access Control Procedures for Users (AC-2).[2] They include account management (AC-2), access enforcement (AC-3), separation of duties (AC-5), least privilege (AC-6), remote access (AC-17), wireless access (AC-18), and access control for mobile devices (AC-19).

8.3. **Information Flow Enforcement (AC-4)**

8.3.1. Information flow within and between State information systems is restricted using technical enforcement mechanisms administered by OIT, including firewalls, routing rules, network segmentation, and approved external connection pathways. OIT applies these mechanisms to prevent unauthorized or unintended information transfer.

8.3.1.1. The flow of information traverses OIT-managed infrastructure assets (firewall, virtual private network (VPN), multilayer switches, and router devices) that use protocols restricting information asset services.

8.3.1.2. The flow of information within systems and between systems is partially controlled through OIT-managed firewalls, with rules that, by default, deny all outside traffic entry to the State network.

8.3.1.2.1. OIT, in collaboration with external entities, establishes dedicated VPNs to control the flow of information to and from approved foreign networks and cloud providers.

8.3.1.2.2. OIT implements demilitarized zones (see Definitions) to limit inbound traffic to information assets that provide authorized, publicly accessible services, protocols, and ports. Inbound internet traffic is limited to internet protocol addresses within the demilitarized zone.

8.3.1.3. The flow of information within systems and between systems is controlled, in part, through OIT-managed routers

[2] https://www.maine.gov/oit/policies/AccessControlProceduresForUsers.pdf

and multilayer switches that use protocols to, by default, deny information asset access.

8.3.1.3.1. Access control lists are utilized to filter and control network traffic and as the basis for flow control decisions.

8.3.1.3.2. Network diagrams that document information asset flow and interconnected systems on the State network are developed and maintained by OIT.

8.3.2. By default, auto-forwarding any Maine.Gov email to a domain other than Maine.Gov is prohibited. Should there be a compelling business reason to do so, the request must be processed through a waiver (see Waiver Policy).[3]

8.4. Unsuccessful Logon Attempts (AC-7, (2))

8.4.1. The State of Maine enforces controls that limit the number of consecutive unsuccessful logon attempts and automatically apply protective actions to reduce the risk of brute-force authentication attacks or credential misuse.

8.4.1.1. A limit of (a defined number) consecutive invalid login attempts by a user, during (a defined time period); and

8.4.1.2. The user is locked out of the account (for a defined duration) when the maximum number of login attempts is exceeded.

8.4.2. Three consecutive invalid login attempts within a 15-minute period produces an account lockout of 15 minutes.

8.4.2.1. These standards are enforced by group policy for all Active Directory users and extend to information assets that utilize Active Directory.

8.4.2.2. Agency information assets that do not leverage Active Directory must use alternative mechanisms to ensure compliance with these standards.

8.4.3. **Purge or Wipe Mobile Device (AC-7 (2)) -** The OIT Mobile Device Policy[4] establishes the requirements for mobile device access to the State network. Mobile devices managed by OIT are wiped after ten (10) consecutive, unsuccessful login attempts.

8.5. System Use Notification (AC-8)

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

8.5.1. System use notifications must be displayed to users before accessing State-managed information systems. OIT and agency partners coordinate to ensure these notifications are consistently implemented across applicable systems.

8.5.1.1. OIT requires an Acceptable Use of State Resources banner (Active Directory banner) be displayed that identifies usage considerations for all local and remote State of Maine domain users.

8.5.1.1.1. The State of Maine requires notice that the system may contain Maine State and U.S. Government information, notice of the pornography restriction, and notice of the incidental-use policy to be in the Active Directory banner.

8.5.1.1.2. The Active Directory banner remains displayed until the user acknowledges the usage conditions prior to State domain access being granted. Acknowledgment can be by clicking an OK button or by pressing the Enter key.

8.5.1.1.3. Where required, OIT systems that do not use Active Directory will display a warning banner that contains the same content as the Active Directory banner. See Appendix A for Approved Warning Banner Language.

8.5.1.2. Agencies identify additional banner requirements, including content and acknowledgement expectations, for agency-managed information assets such as business applications and publicly accessible systems.

8.5.1.2.1. OIT asset owners implement, where technically possible and to the extent possible, identified agency banners, banner content, and user acknowledgement.

8.5.1.2.2. This includes banners for end users (such as business application users) and banners for privileged users (see Definitions) (for example, database, server, operating system, and network administrators).

8.6. **Concurrent Session Control (AC-10) -** Agencies determine whether additional concurrent session controls are needed for agency-managed information assets and document such requirements accordingly.

8.7. **Session Lock (AC-11, (1))**

8.7.1. Agencies, in collaboration with OIT, ensure that required device-lock controls for agency information assets are implemented.

8.7.2. OIT initiates a device lock after 15 minutes of inactivity, or upon receiving a request from a user. This standard is enforced by group policy for all Active Directory users.

8.7.2.1. The device lock is maintained until the user reestablishes access by providing identification and authentication credentials.

8.7.3. Agencies, in collaboration with OIT, ensure that the information asset device lock conceals information visible on the display by replacing it with a publicly viewable image.

8.7.4. The OIT enforces a screen lock policy across all managed devices to ensure that information visible on the screen is concealed when the device is locked or inactive.

8.7.4.1. Upon activation of the device lock, the display is replaced with a publicly viewable image such as a screensaver, solid color, clock, or blank screen.

8.7.4.2. For Microsoft Windows systems, this is applied through a Group Policy Object (GPO) for all Active Directory (AD) users, with equivalent configurations managed through Mobile Device Management (MDM) solutions or native settings for other supported platforms.

8.8. Session Termination (AC-12, (1), (2), (3))

8.8.1. Agencies identify session termination requirements for their information assets in alignment with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

8.8.2. OIT implements user session termination at the information asset level. For example, secure file transfer protocol, Unix, and network all have session termination controls in place, whereby all processes associated with a user's logical session (except processes specifically created by the user to continue after the session) are terminated after fifteen minutes of inactivity.

8.8.3. **User-Initiated Logouts (AC-12(1)) –** OIT ensures that authenticated users can intentionally terminate their sessions through a clear and secure logout capability wherever required.

8.8.4. **Session Termination Messages (AC-12(2)) –** OIT ensures that all managed systems and applications provide clear indication to users when an authenticated session has ended.

8.8.4.1. This notification may be explicit, such as a logout or timeout message, or implicit, such as returning the user to a login screen or access denial page.

8.8.4.2. The intent is to ensure users understand that the authenticated communication session has been terminated and that access to protected resources requires re-authentication.

8.8.5. **Timeout Warning Messages (AC-12(3)) –** Session termination behavior is configured by OIT in accordance with established security parameters.

8.8.5.1. Systems are designed to indicate when an authenticated session has ended, either implicitly or explicitly.

8.8.5.2. Agencies may request additional user notifications, such as pending session termination warnings, if operationally beneficial.

8.8.5.3. Requests or modifications to these configurations are managed through OIT's established change management processes (see Change Management Policy And Procedures[5]) .

8.8.5.4. These configurations primarily address user behavior and awareness rather than system security controls.

8.8.6. For information assets where OIT has control of the code, OIT application owners implement required agency-identified session termination controls at the application level.

8.9. **Permitted Actions Without Identification or Authentication (AC-14)**

8.9.1. Agencies identify and appropriately document actions that can be performed on agency information assets and agency websites without identification or authentication that are consistent with organizational missions and business functions and with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

8.9.2. The following do not currently require identification or authentication:

8.9.2.1. By statute,[6] the Maine.gov portal is open to the public by default.

8.9.2.1.1. Depending on the sensitivity of content and functionality offered, agencies may elect to require authentication and/or identification for

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf
[6] https://legislature.maine.gov/legis/statutes/1/title1sec536.html

access to agency information assets and agency websites.

8.9.2.2. Agencies, in collaboration with OIT, manage several sets of publicly accessible devices. These include, but are not limited to:

8.9.2.2.1. Department of Health and Human Services - My Maine Connection public devices;

8.9.2.2.2. Maine State Library public devices; and

8.9.2.2.3. Department of Labor Career Center public devices.

8.9.2.3. OIT does not verify phone calls. The State of Maine does not transact business based solely on caller identity.

8.10. Security and Privacy Attributes (AC-16)

8.10.1. Data classification supports the protection and proper handling of information throughout its lifecycle. OIT establishes the enterprise framework in the OIT Data Classification Policy[7], which governs how data is labeled, marked, and protected across enterprise systems, while agencies retain ownership of their data and associated privacy obligations.

8.10.2. Attribute audit requirements are detailed in the Audit and Accountability Policy and Procedures (AU)[8] and supported by OIT's enterprise auditing and monitoring systems.

8.11. Use of External Information Assets (AC-20, (1), (2), (3))

8.11.1. **External System Conditions (AC-20) -** OIT defines and enforces the conditions under which external systems may connect to or interact with State of Maine information systems to ensure protection of State data and resources. The following highlights representative baseline controls and practices as examples of implementation.

8.11.1.1. External Access Management - Access to the State of Maine network from external systems is permitted only through a managed VPN solution that enforces authentication, device compliance, and configuration standards prior to connection. Due to its prevalence, it is also worth noting that access to State of Maine Microsoft Azure environments is similarly protected under the controls and assurances of Microsoft's Federal Risk and Authorization Management

[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AuditAccountabilityPolicyProcedures.pdf

Program (FedRAMP) certification, ensuring consistent security governance across cloud-hosted systems.

8.11.1.2. Data Sensitivity and FIPS 199 Categorization - Federally regulated or otherwise sensitive data is not accessible from external systems unless explicitly determined to be public or authorized by the owning agency in accordance with applicable regulatory requirements. The maximum security category of information processed, stored, or transmitted from external systems is governed by the agency's data classification policy which is heavily influenced by the Federal Information Processing Standards (FIPS) Publication 199 categorization.

8.11.1.3. Network and System Protections - OIT employs a layered security architecture consisting of hardware appliances, software controls, and continuous monitoring tools to enforce access restrictions, detect anomalies, and alert security personnel. These protections are generally agnostic to the means of connection and apply across State of Maine issued devices, wireless technologies, and connections provided by other Internet Service Providers (ISPs).

8.11.1.4. Endpoint and Threat Protection - Endpoint protection is maintained through managed security agents and supporting technologies (e.g., Domain-based Message Authentication, Reporting, and Conformance (DMARC)). This includes malware and threat protection tools for virus and spyware defense.

8.11.1.5. Physical Security - Physical security controls are implemented throughout the enterprise including badge readers, surveillance systems, and contracted security or law enforcement personnel to prevent unauthorized physical access to information systems.

8.11.1.6. Maintenance and Updates - Updates to security technologies, software, and configurations are executed through OIT's continuous improvement and change management processes, occurring at intervals driven by vendor patching cycles, operational priorities, and threat intelligence assessments.

8.11.1.7. These controls and practices are detailed across the full set of security control family policy and procedure documents, which collectively define the enterprise-level policies, standards, and implementation methods. Taken together,

these documents constitute the preponderance of the System Security Plan (SSP) details for the enterprise.

8.11.2. **Authorized Use of External Information Assets (AC-20(1)) -** Agencies, in collaboration with OIT, permit authorized individuals to use an external information asset to access the information asset or to process, store, or transmit agency-controlled information only when the implementation of required security controls is verified or when approved information asset connection or processing agreements are in place that are consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

8.11.2.1. OIT has a detailed Remote Hosting Policy**Error! Bookmark not defined.** that establishes default requirements and responsibilities for remote-hosted State of Maine information assets.

8.11.3. **Use of Portable Storage Devices on External Information Assets (AC-20(2)) -** Agencies, in collaboration with OIT, restrict the use of agency-controlled portable storage devices by authorized individuals on external information assets, as consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

8.11.3.1. By default, OIT does not implement portable storage device restrictions but has the capability to implement agency-defined restrictions for the information assets it manages.

8.11.4. **Restrictions on Non-Organizationally Owned Information Assets (AC-20(3)) -** Agencies, in collaboration with OIT, restrict the use of nonorganizationally owned information assets, or devices to process, store, or transmit agency information, as is consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

8.11.4.1. The OIT Mobile Device Policy[9] prohibits State of Maine employees and contractors from connecting any new personal devices (see Definitions) not owned by the State of Maine or an approved vendor to any State of Maine system for any reason (for example, charging, data transfer, internet access).

8.12. **Information Sharing (AC-21)**

8.12.1. Agencies must establish processes to approve access to systems and restricted data types and ensure that personnel are trained on the appropriate handling and sharing of information. OIT supports these agency access processes through Active Directory (AD) controls and

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

individual application access managed through the Information Technology Service Management (ITSM) system.

8.12.2. OIT documents system interconnections with vendors and external entities using Service Level Agreements (SLAs), Data Exchange Agreements (DUAs), and contracts, as outlined in the Security Assessment and Authorization Policy and Procedures (CA)[10]. These documents collectively define approved data sharing, access authorizations, and technical safeguards governing external information exchange.

8.12.3. OIT also reinforces proper information-sharing behavior through Security Awareness and Training (AT) activities, as detailed in the Security Awareness and Training Policy and Procedures (AT)[11], which ensure that all personnel understand data-sharing responsibilities and applicable restrictions.

8.12.4. See the Data Exchange Policy[12] for additional information on approved data-sharing mechanisms and requirements.

8.12.5. Authorized users of a particular data type may share data only with other individuals, groups, and organizations authorized to receive that data type.

8.13. Publicly Accessible Content (AC-22)

8.13.1. In managing publicly accessible content, agencies:

8.13.1.1. Designate personnel authorized to post information onto a publicly accessible agency information asset;

8.13.1.2. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

8.13.1.3. Review the proposed content of information prior to posting onto the publicly accessible information asset to ensure that nonpublic information is not included; and

8.13.1.4. Review the content on the publicly accessible information asset for nonpublic information at agency-defined intervals and remove any nonpublic information.

[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityAssessmentAuthorizationPolicy.pdf
[11] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityAwarenessTrainingPolicy.pdf
[12] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf

8.13.2. Agencies designate webmasters or web coordinators to manage the publicly accessible content on their agency websites. See the InforME Network Services Policy[13] and the Web Standards.[14]

8.13.2.1. Agencies authorize these individuals, and InforME grants agency-authorized access for agency personnel who manage publicly accessible content on the Maine.gov portal.

8.14. **Data Mining Protection (AC-23)**

8.14.1. OIT monitors for anomalous or suspicious data access activities that may indicate large-scale or unauthorized data mining.

8.14.2. Security monitoring and alerting systems detect unusual patterns of data access or aggregation and escalate them for investigation to protect State information assets.

9.0. Document Details

9.1. Initial Issue Date: August 19, 2019

9.2. Latest Revision Date: January 16, 2026

9.3. Point of Contact: PolicyTeam.OIT@Maine.Gov

9.4. Approved By: Chief Information Officer, OIT

9.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[15]

9.6. Waiver Process: Waiver Policy[16]

9.7. Distribution: Internet[17]

10.0. Review

This document will be reviewed triennially, 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 *Major Administrative Policies and Procedures* and *Internal Control Policies and Directives* records management categories. They will be retained for a minimum of six years after withdrawal or replacement and then destroyed in accordance with guidance[18] provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

---

[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/InforMENetworkServicesPolicy.pdf
[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/WebStandards.pdf
[15] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[16] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[17] https://www.maine.gov/oit/policies-standards
[18] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf

12.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA),[19] 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 Maine State 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. Access Approval Process: The method by which a user's request for access to an information asset is reviewed, verified, and authorized in accordance with applicable policy and least-privilege principles.

13.2. Access Control List (ACL): A ruleset applied to network devices, systems, or applications to permit or deny communication based on defined criteria such as protocol, port, source address, or destination address.

13.3. Access Control: The process of granting or denying specific requests to 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (for example, Federal buildings, military establishments, border crossing entrances).

13.4. Active Directory (AD): The State of Maine's enterprise directory service that provides centralized authentication, authorization, account management, and policy enforcement.

13.5. Agency Data Custodian: Agency official, who, based on his or her position, is a 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 Department of Health and Human Services Office of Family Independence Director (or designee) is the Agency Data Custodian for Benefits Information Assets.

13.6. Application Owner: The individual within the OIT responsible for the management, security, and operational oversight of specific information assets or applications.

13.7. Authentication: The process of verifying the identity of a user, process, or device as a prerequisite to granting access to an information asset.

13.8. Authorization: The process of granting an authenticated user permission to access specific information, systems, or services based on approved rights and privileges.

13.9. Authorized User: An individual who has approved access to an information asset to perform job responsibilities.

[19] https://legislature.maine.gov/statutes/1/title1sec402.html

13.10. Availability: Timely and reliable access to and use of information assets.

13.11. Boundary Protection: The set of controls used to monitor and restrict information flow across network boundaries and security domains.

13.12. Confidentiality: The state of being kept private or secret, including preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

13.13. Compensating Controls: Alternative security controls used to satisfy a requirement when the primary control cannot be implemented due to operational or technical limitations.

13.14. Controlled Unclassified Information (CUI): Information that requires safeguarding or dissemination controls pursuant to applicable law, regulation, or government-wide policy, but is not classified.

13.15. Data Mining: The automated or large-scale analysis of data sets to discover patterns, relationships, or anomalies that may indicate unauthorized access or misuse.

13.16. Demilitarized Zone (DMZ): A host or network segment inserted as a "neutral zone" between an organization's private network and the internet.

13.17. Foreign Remote Access: A less common and unusual variety of Remote Access, where State of Maine personnel remotely access State of Maine information asset(s) from a location outside the United States, U.S. territories, embassies, or military installations.

13.18. Group Policy Object (GPO): A configuration management mechanism used within AD to enforce security settings and standardize system behavior.

13.19. Human Resources Management System (HRMS): The system used by the State of Maine to manage personnel records and processes, including automated account provisioning.

13.20. Identity and Access Management: The set of processes used to establish user identity, assign and manage access rights, and control authentication and authorization.

13.21. Incident Response: The actions taken to detect, analyze, contain, remediate, and recover from a cybersecurity or operational incident.

13.22. Information Assets: Used interchangeably with Information Systems. 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. (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30).

13.23. Information Technology Service Management (ITSM): The formalized framework through which OIT manages service requests, incident resolution, change management, and access approval.

13.24. In-State Remote Access: The more common, and default, variety of Remote Access, where State of Maine personnel remotely access State of Maine information asset(s) from a location inside the State of Maine, but outside a State of Maine office location.

13.25. Integrity: The accuracy and consistency (validity) of data over its lifecycle. Guarding the integrity of information assets against improper modification or destruction includes ensuring information nonrepudiation and authenticity.

13.26. Logical Session: A user-initiated interaction with a system that begins at authentication and ends when the user logs out, or the system terminates the session.

13.27. Long-term: 30 days or more.

13.28. Mobile Device Management (MDM): Technology used to manage, secure, configure, and monitor mobile devices used to access State information assets.

13.29. Nonpublic Information: Information that is not authorized for public release, including confidential, sensitive, proprietary, or legally restricted data.

13.30. Out-of-State Domestic Remote Access: A less common variety of Remote Access, where State of Maine personnel remotely access State of Maine information asset(s) from a location outside the State of Maine, but within the United States, including U.S. territories, embassies, and military installations.

13.31. Personal Devices: Portable storage media, mobile computing devices, or any personal technology capable of storing, transmitting, or receiving information. Include the following categories:

13.31.1. Portable cartridge or disk-based, removable storage media (for example, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards or drives that contain nonvolatile memory).

13.31.2. Portable computing and communication devices with information storage capability (for example, notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices); and

13.31.3. Any other mobile computing device small enough to be easily carried by an individual, able to wirelessly transmit or receive information, and have local, nonremovable data storage and a self-contained power source.

13.32. Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity.

13.33. Principle of Least Privilege: A security principle whereby users are assigned the minimum access necessary to perform their job responsibilities. Access is granted for the shortest duration possible.

13.34. Privileged User: A user who is granted rights that go beyond those of a typical business user to manage and maintain IT systems. Usually, these rights include administrative access to networks and devices and are separate from users' administrative access to their own workstations.

13.35. Remote Access: Access to State information assets initiated from outside a State of Maine office location.

13.36. Separation of Duties: A security principle that divides critical functions among staff members to ensure that no one individual has enough information or access privileges to perpetrate damaging fraud (i.e., no user should be given enough privileges to misuse the system on their own).

13.37. Service Level Agreement (SLA): A formal agreement describing expected service performance, responsibilities, and security requirements between parties.

13.38. Session Termination: A system-enforced end to a logical session due to user logout, timeout, or security controls.

13.39. Short-Term: Fewer than 30 days.

13.40. Trust Relationship: A formal or implicit agreement defining the level of assurance between organizations, permitting limited reliance on each other's security controls.

14.0. Abbreviations

14.1.	ACL:	Access Control List
14.2.	AD:	Active Directory
14.3.	AT:	Awareness and Training
14.4.	CA:	Security Assessment and Authorization
14.5.	CISO:	Chief Information Security Officer
14.6.	CUI:	Controlled Unclassified Information
14.7.	DAFS:	Department of Administrative and Financial Services
14.8.	FOAA:	[Maine] Freedom of Access Act
14.9.	GPO:	Group Policy Object
14.10.	HRMS:	Human Resources Management System
14.11.	ISO:	OIT Information Security Office
14.12.	ITSM:	Information Technology Service Management
14.13.	MOA:	Memorandum of Agreement
14.14.	NIST:	National Institute of Standards and Technology
14.15.	OIT:	[Maine] Office of Information Technology
14.16.	PII:	Personally Identifiable Information

14.17. SLA: Service Level Agreement

14.18. VPN: Virtual Private Network

Appendix A: Approved Warning Banner Language

Used for systems that do not have space constraints for the banner. Banner displayed at sign-on to a State of Maine computer:

This is a Maine State Government computer system. It may contain Maine State and U.S. Government information. This system, and all related equipment and network, including access to the internet, are provided for authorized Maine State Government use ONLY. Any personal use must be of an incidental nature and not interfere with Maine State Government business. Unauthorized access, use, misuse, or modification of this system is strictly prohibited and may subject you to state and federal criminal prosecution and penalties, as well as civil penalties and other adverse administrative action. These systems are monitored and audited for many purposes, including protecting against unauthorized usage and ensuring the security and optimal functioning of the Maine State Government network. At any time, the government may intercept, search, and seize any communication or data transiting or stored on this system. By using this system, you are consenting to system monitoring for law enforcement and other purposes.

State employees shall NOT use Maine State Government computer systems to access, or download, or otherwise view, or transmit, pornographic material. This prohibition applies irrespective of whether the employee is on or off-duty, and regardless of whether the access is incidental in nature. Violation of this work rule constitutes just cause for dismissal from employment.

SELECTING PROCEED CONSTITUTES ACCEPTANCE OF TERMS OF USE.

Banner for systems that have limited display space:

WARNING! THIS SYSTEM CONTAINS U.S. GOVERNMENT INFORMATION. BY ACCESSING AND USING THIS COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO STATE AND FEDERAL CRIMINAL PROSECUTION AND PENALTIES AS WELL AS CIVIL PENALTIES.

Appendix B for Approved Public Wi-Fi Use Banner Language

You may not use the State of Maine's Public Wi-Fi Network without agreeing to these Terms and Conditions. By clicking [ACCEPT] and connecting to this State of Maine Public Wi-Fi Network, you acknowledge and consent to the following:

TERMS AND CONDITIONS

This is a State of Maine Public Wi-Fi Network provided for public use. Users have NO EXPECTATION OF PRIVACY in the use of this Network. All communications and data transiting, traveling to or from, or stored on this Network will be monitored. By accessing this Network, you consent to the unrestricted monitoring, interception, recording, and searching of all communications and information transiting, traveling to or from, or stored on this Network at any time and for any purpose by the State of Maine and by any person or entity, including law enforcement or other state or federal government entities. You also consent to the unrestricted retrieval and disclosure of all communications and information transiting, traveling to or from, or stored on this Network at any time and for any purpose by the State of Maine and by any person or entity, including law enforcement or other state or federal government entities.

State of Maine personnel cannot use this Network for any official state business. You agree not to use this Network to engage in any unlawful activity, attempt unauthorized access to State systems, access, view, or obtain obscene materials, or transmit harmful or malicious content. Such use of this Network is strictly prohibited and may be subject to criminal prosecution. As this is an unsecured public Network, users are responsible for their own Internet safety. There is no assurance of network compatibility or availability. Users are responsible for protecting their own devices and information and are advised to protect themselves from viruses, computer worms, spyware, malware, scams, identity theft and malicious monitoring. The State of Maine does not undertake the security of any information sent through the Network, and is not responsible for any loss, theft, interception, or compromise of information that may occur while using the Network.

These acknowledgments and consents cover all use of the State of Maine Public Wi-Fi Network, including work-related use and personal use without exception.