State of Maine
Department of Administrative and Financial Services
Office of Information Technology

Access Control Policy and Procedures (AC-1)

Table of Contents

1.0. Document Purpose

The purpose of this document is to define the State of Maine policy and procedures for implementing and maintaining appropriate access controls (see Definitions) for State information assets (see Definitions). This document corresponds to the Access Control Control Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

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.

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 Sytem; and

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

4.2. Chief Information Security Officer

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. Department of Administrative and Financial Services Bureau of Human Resources
4.3.1. 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).

4.4. OIT
4.4.1. Assigns an owner for each information asset supported by OIT.

4.5. OIT Information Asset Owners
4.5.1. Ensure that authorized personnel access to assigned assets is based on the principle of least privilege;
4.5.2. In collaboration with IT procurement and agencies, hold contracted other parties that host State information assets accountable to this Policy and Procedures; and
4.5.3. 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.

4.6. IT Procurement
4.6.1. In collaboration 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 procedures that support it.

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 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

7.0. For State of Maine employees, failure to comply with this document may result in progressive discipline, up to and including dismissal.

7.1. 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.

7.2. 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 procedures serve as the base requirements for State of Maine information assets. They represent the security controls established to provide an acceptable level of protection from unauthorized system access.

8.1. Access Control Procedures for Users

8.1.1. User access control procedures are identified separately in Access Control Procedures for Users (AC-2).[1] 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).

8.2. Information Flow Enforcement (AC-4)

8.2.1. Agencies, in collaboration with OIT, ensure that agency information assets enforce approved authorizations for controlling the flow of information within the system and between interconnected systems that are consistent with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

8.2.1.1. 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.

8.2.1.2. 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.

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

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

8.2.1.2.2. 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.

8.2.1.3. The flow of information within systems and between systems is controlled, in part, through OIT-managed routers and multilayer switches that use protocols to, by default, deny information asset access.

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

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

8.2.2. 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).[2]

8.3. Unsuccessful Logon Attempts (AC-7)

8.3.1. Agencies, in collaboration with OIT, ensure that agency information assets enforce the following rules, with the number, time-period, and duration of events defined in accordance with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance:

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

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

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

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

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

8.4. System Use Notification (AC-8)

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

8.4.1. Agencies, in collaboration with OIT, ensure that a system use notification is displayed to users and that it is consistent with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance,

8.4.1.1. 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.

8.4.1.1.1. 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.

8.4.1.1.2. 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.

8.4.1.1.3. 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.

8.4.1.2. Agencies define required banners, banner content, and user acknowledgement for their agency information assets (including publicly accessible systems) and associated components to be consistent with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

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

8.4.1.2.2. 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).

8.5. Concurrent Session Control (AC-10)

8.5.1. Agencies identify any required concurrent session controls for agency information asset end users that are consistent with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

8.6. Session Lock (AC-11, AC-11(1))

8.6.1. Agencies, in collaboration with OIT, ensure that required device-lock controls for agency information assets are implemented and are consistent with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

8.6.2. 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.

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

8.6.3. 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.

8.6.4. OIT implements a screen saver group policy for all Active Directory users, whereby the information visible on the screen is concealed and replaced with a publicly viewable image when the device lock is activated.

8.7. Session Termination (AC-12)

8.7.1. Agencies define session termination requirements for their agency information assets that are consistent with applicable Federal laws, executive orders, directives, policies, regulations, standards, and guidance.

8.7.2. 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.

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

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

8.8.1. 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.

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

8.8.2.1. By statute,[3] the Maine.gov portal is open to the public by default.

8.8.2.1.1. Depending on the sensitivity of content and functionality offered, agencies may elect to require authentication and/or identification for access to agency information assets and agency websites.

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

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

[3] https://legislature.maine.gov/legis/statutes/1/title1sec536.html

8.8.2.2.2. Maine State Library public devices; and
8.8.2.2.3. Department of Labor Career Center public devices.
8.8.2.3. OIT does not verify phone calls. The State of Maine does not transact business based solely on caller identity.

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

8.9.1. Agencies, in collaboration with OIT, ensure that terms and conditions established are consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information assets, allowing authorized individuals to:
8.9.1.1. Access the information asset from external information assets; and
8.9.1.2. Process, store, or transmit agency-controlled information, using external information assets.
8.9.1.3. OIT has a detailed Remote Hosting Policy[4] that establishes requirements and responsibilities for remote-hosted State of Maine information assets.

8.9.2. 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.
8.9.2.1. OIT has a detailed Remote Hosting Policy[4] that establishes default requirements and responsibilities for remote-hosted State of Maine information assets.

8.9.3. 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.
8.9.3.1. 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.

8.9.4. 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.
8.9.4.1. The OIT Mobile Device Policy[5] prohibits State of Maine employees and contractors from connecting any new personal devices (see

[4] https://www.maine.gov/oit/policies/RemoteHostingPolicy.pdf
[5] https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf

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).

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

8.10.1. Agencies, in collaboration with OIT, ensure any information sharing includes protections consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. See the Data Exchange Policy[6] for additional information.

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

8.11. **Publicly Accessible Content (AC-22)**

8.11.1. In managing publicly accessible content, agencies:

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

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

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

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

8.11.2. Agencies designate webmasters or web coordinators to manage the publicly accessible content on their agency websites. See the InforME Network Services Policy[7] and the Web Standards.[8]

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

9.0. Document Details

9.1. Initial Issue Date: August 19, 2019
9.2. Latest Revision Date: July 24, 2024
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[9]
9.6. Waiver Process: Waiver Policy[10]

---

[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf
[7] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/InforMENetworkServicesPolicy.pdf
[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/WebStandards.pdf
[9] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf

9.7. Distribution: Internet[11]

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 *Routine Administrative Policies and Procedures* and *Internal Control Policies and Directives* records management categories. They will be retained for a minimum of 6 years after withdrawal or replacement and then destroyed in accordance with guidance[12] 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 (FOAA),[13] certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as to 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 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).

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

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

---

[11] https://www.maine.gov/oit/policies-standards
[12] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf
[13] https://legislature.maine.gov/statutes/1/title1sec402.html

13.4. Demilitarized zone: A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet.

13.5. 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.

13.6. Information assets: The full spectrum of all information technology products, including business applications, system software, development tools, utilities, appliances, and so forth.

13.7. 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.

13.8. Long-term: 30 days or more.

13.9. 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.

13.10. Personal devices: Include the following categories:
- 13.10.1. 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);
- 13.10.2. 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
- 13.10.3. Any other mobile computing device small enough to be easily carried by an individual, able to wirelessly transmit or receive information, and having local, nonremovable data storage and a self-contained power source.

13.11. 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.

13.12. 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.

13.13. Separation of duties: A security principle that divides critical functions among staff members to ensure that no one individual has enough information or access

privilege to perpetrate damaging fraud (i.e., no user should be given enough privileges to misuse the system on their own).

13.14. Short-Term: Fewer than 30 days.

14.0. Abbreviations

14.1. FOAA: [Maine] Freedom of Access Act
14.2. OIT: Office of Information Technology
14.3. VPN: Virtual Private Network

Appendix A for 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.