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

Access Control Procedures for Users (AC-2, 3, 5, 6, 17, 18, & 19)

Table of Contents

1.0. Purpose

These procedures identify how the State of Maine meets security requirements pertaining to account management, access enforcement, separation of duties, least privilege, remote access, wireless access, and access control for mobile devices. This document corresponds to the Controls AC-2, 3, 5, 6, 17, 18 and 19 of the Family of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0. Scope

2.1. These procedures apply 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 (see Definitions), irrespective of location; and
- 2.1.2. Information assets from other State government branches that use the State network.

3.0. Procedure Conflict

If these procedures conflict with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0. Procedures

4.1. The following procedures serve as the base set of requirements for State of Maine information assets. They represent the security controls that have been established to provide protection from unauthorized system access.

4.2. Account Management (AC-2, AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(7))

- 4.2.1. The Office of Information Technology (OIT) ensures that information asset accounts are identified and selected to support agency missions and business functions in a manner that is consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
  - 4.2.1.1. OIT uses the following types of authorized user accounts:
    - 4.2.1.1.1. Individual accounts;
    - 4.2.1.1.2. Role-based shared accounts;
    - 4.2.1.1.3. Group accounts; and
    - 4.2.1.1.4. System accounts.

- 4.2.2. Agencies must assign gatekeepers to manage agency information asset account authorizations.
  - 4.2.2.1. OIT utilizes the Numara Footprints IT Service Management (Footprints) application to manage user account requests (establish, modify, or terminate user access accounts).
  - 4.2.2.2. Authorized agency personnel submit user account requests via the Footprints user request web form, providing all required information and justification for the request.

4.2.2.2.1. The request is assigned to the appropriate OIT information asset owners (for example, Active Directory and File Services team for Active Directory accounts) for fulfillment.

4.2.2.2.2. The OIT assignee updates the request to notify the agency when the request is fulfilled.

4.2.3. Agencies must establish conditions for group and role membership by specifying authorized users of the information asset, group and role membership, and access authorizations (i.e.,privileges) and other attributes (as required) for each account;

4.2.3.1. Authorized agency personnel provide approval and specify this information in the Footprints ticket user access request to OIT.

4.2.3.2. Agencies utilize established OIT standards and Footprints tickets, to create, enable, modify, disable, and remove accounts for each account type. These procedures include the following activities:

4.2.3.2.1. Authorizing access to the information asset based on:

4.2.3.2.1.1. A valid access authorization;

4.2.3.2.1.2. Intended system usage; and

4.2.3.2.1.3. Other attributes as required by the organization or associated missions/business functions;

4.2.3.3. Agencies must monitor the use of agency information asset accounts and notify OIT through the Footprints ticketing system when:

4.2.3.3.1. Accounts are no longer required;

4.2.3.3.2. Personnel are terminated or transferred; and

4.2.3.3.3. Personnel information asset usage or need-to-know changes.

4.2.3.4. Agencies must establish a process for reissuing shared and group account credentials (if deployed) when individuals are removed from the group.

4.2.4. OIT employs the automated mechanisms that come with Active Directory to support account management.

4.2.5. OIT does not automatically disable temporary or service accounts after a set duration. Rather, OIT provides inactive account reports to agencies on a monthly basis through the Account Managers.

4.2.6. OIT does not automatically audit account creation, modification, enabling, disabling, and removal actions; however, OIT does perform all such functions upon request.

4.2.7. OIT follows role-based access for privileged administrator accounts.

4.3. Access Enforcement (AC-3, AC-3(9))

4.3.1. Agencies must ensure that agency information assets enforce approved authorizations to information and system resources, in accordance with applicable access control policies and in a manner that is consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.3.1.1. OIT requires that access to any State information asset must be made by authorized agency personnel.

4.3.1.1.1. Authorized agency personnel utilize the Footprints ticketing system user request workspace to initiate new user-access requests.

4.3.1.1.2. Any change to established user access (modified access, terminated access) must be requested through the Footprints user request workspace by authorized agency personnel.

4.3.1.2. OIT requires that access to any State information asset be based on each user's access privileges. This access may be restricted by day, date, and time, as appropriate.

4.3.1.3. For the information assets it supports, OIT does not release information outside of the established system boundary unless:

4.3.1.3.1. The receiving organization information asset or system component provides agency-defined security safeguards; and

4.3.1.3.2. The agency-defined safeguards are used to validate the appropriateness of the information designated for release.

4.4. Separation of Duties (AC-5)

4.4.1. Both the agencies and OIT identify any required separation of duties for their agency information assets, consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Examples include:

4.4.1.1. Ensuring that audit functions are not performed by personnel responsible for administering access control;

4.4.1.2. Maintaining a limited group of administrators with access based on the users' roles and responsibilities;

4.4.1.3. Ensuring that critical mission functions and information asset support functions are divided among separate individuals;

4.4.1.4. Ensuring that information asset testing functions (for example, user acceptance, quality assurance, and information security) and production functions are divided among separate individuals or groups; and

4.4.1.5. Ensuring that an independent entity, not the business owner, system developer(s) or maintainer(s), or system administrator(s) responsible for the information asset conducts information security testing of the information asset.

4.4.2. Both the agencies and OIT must ensure that, where required, separation of duties of personnel is documented and that information asset access authorizations to support separation of duties are defined.

4.4.2.1. Agencies collaborate with the application development managers and account managers to implement agency-identified, required information asset separation of duties for OIT-managed systems.

4.5. Least Privilege (AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10))

4.5.1. Both the agencies and OIT must ensure that the principle of least privilege is employed for agency information assets to ensure that users (or processes acting on behalf of users) are allowed only authorized access necessary to accomplish assigned tasks, in accordance with job duties, consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.5.1.1. For the information assets it supports, OIT employs the principle of least privilege, which allows authorized access for users (or processes acting on behalf of users) only as necessary for the user to accomplish assigned tasks in accordance with job duties.

4.5.1.2. OIT explicitly authorizes access to system utilities by requiring that they be made available only to those with a legitimate business case.

4.5.1.3. OIT requires that system administration accounts (for example, root access) be limited to the smallest group possible and be subject to the principle of least privilege.

4.5.1.4. OIT requires that administrators first login as themselves (ordinary user) before escalating privileges to the level of an administrator.

4.5.1.5. OIT implements safeguards to prevent non-privileged users of information assets from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards or countermeasures.

4.5.2. OIT restricts privileged accounts on the information asset to defined personnel or roles (defined in the applicable security plan).

4.5.3. OIT audits the execution of privileged functions.

4.5.4. All OIT-supported information assets prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards or countermeasures.

4.6. Remote Access (AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4))

4.6.1. Both the agencies and OIT must ensure that usage restrictions, configuration and connection requirements, and implementation guidance for remote access to agency information assets is established and that remote access is authorized prior to allowing connections, consistent with applicable federal

laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.6.1.1. OIT requires that remote access occurs via established virtual private networks (VPNs) utilizing multifactor authentication host verification (host operating system checker and anti-malware).

4.6.1.2. Secure tokens, assigned to specific individuals, are required for remote access. These secure tokens are issued by OIT upon receipt of a request from authorized agency personnel.

4.6.1.3. Office 365 leases that allow remote access by trusted devices are granted for 30 days. Each time a device connects to the internal network, the lease is renewed.

4.6.1.4. OIT monitors and controls remote access, using a secure portal with automated, standard reporting capabilities.

4.6.1.4.1. Administrative tools are used to kill rogue connections that are identified.

4.6.1.5. OIT utilizes end-to-end VPN encryption to protect the confidentiality and integrity of remote connections.

4.6.1.6. OIT utilizes two distinct, dedicated domain entry points to route all remote access.

4.6.1.7. OIT authorizes the execution of privileged commands and access to security information based on the role of the user, factoring in compelling operational need.

4.6.1.7.1. Given that authorization is role-based, the user has the same privileges regardless whether remote or on-premises.

4.6.1.7.2. Authorized access is documented.

4.6.1.8. OIT requires that all devices that access the State network meet the following security safeguards:

4.6.1.8.1. Up-to-date system patches;

4.6.1.8.2. Current anti-malware; and

4.6.1.8.3. Automatic code execution disabled.

4.7. Wireless Access (AC-18, AC-18(1))

4.7.1. Both the agencies and OIT must ensure that usage restrictions, configuration and connection requirements, and implementation guidance for wireless access to agency information assets is established and that wireless access is authorized prior to allowing connections, consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.7.1.1. OIT requires that agencies comply with the wireless access methods provided by OIT when accessing the State network. Wireless access points are:

4.7.1.1.1. SOM AIRE: The State of Maine's secured wireless network, two-factor authentications: Certificate and Active Directory credentials;

4.7.1.2. SOM GUEST is the wireless network for temporary, incidental connection of vendors, contractors or business partners. It is not intended to be used for connection of guests for more than 6 days, nor to be used to self-sponsored personal devices. User audits identifying "permanent type" connections on SOM GUEST can lead to charges of network access rates to the agency. OIT strictly prohibits the installation of wireless access points that are not managed by OIT.

4.7.1.3. The following restrictions and access controls are integral to all wireless service:

4.7.1.3.1. Encryption protection is enabled;

4.7.1.3.2. SOM AIRE access points are placed in secure areas;

4.7.1.3.3. A firewall is implemented between public access and the entire network;

4.7.1.3.4. Organizational policy related to wireless client access configuration and use is documented by OIT;

4.7.1.3.5. Wireless intrusion and detection system(s) are employed.

4.7.1.4. OIT employs compensating controls in lieu of select wireless access controls as follows:

4.7.1.4.1. Access points are not shut down when not in use but instead are set to degrade off-hours;

4.7.1.4.2. Machine (MAC) address authentication does not take place; instead Active Directory authentication is utilized;

4.7.1.4.3. Static IP addresses are not used for client devices; instead Dynamic Host Configuration Protocol is utilized; and

4.7.1.4.4. Wireless activity monitoring, recording, and review, is not conducted on a regular basis; instead, OIT has overall monitoring, recording, and review that extends to wireless.

4.7.1.5. Wireless access is protected using authentication and encryption.

4.7.1.6. OIT uses Dynamic Host Configuration Protocol (DHCP) for streamlining deployment and increased security. DHCP allows the wireless access points to be sent to the field without being pre-provisioned or primed. The wireless access points are lightweight and cannot be accessed until administrative credentials are pushed to them from the controller. This procedure was approved for use by the IRS instead of using Static IP addresses.

4.7.1.7. See System and Information Integrity Policy,[1] Information System Monitoring (SI-4) for more details.

4.8. Access Control for Mobile Devices (AC-19, AC-19(5), AC-19(7), AC-19(2))

4.8.1. Both the agencies and OIT must ensure that usage restrictions, configuration and connection requirements, and implementation guidance for mobile device access to agency information assets is established and that wireless

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

access is authorized prior to allowing connections, consistent with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Such rules apply irrespective of whether the mobile device is issued by the State or is personally owned.

4.8.1.1. The OIT Mobile Device Policy[2] establishes the requirements for mobile device access to the State network. These requirements include, but are not limited to:

4.8.1.1.1. Authorization requirements for mobile device access to the State network;

4.8.1.1.2. Mobile device encryption requirements to protect confidentiality and integrity, consistent with the sensitivity of the data stored;

4.8.1.1.3. Mobile device management software requirements.

4.8.1.2. Additionally, OIT:

4.8.1.2.1. Monitors for unauthorized connections of mobile devices to information assets;

4.8.1.2.2. Enforces requirements for the connection of mobile devices to information assets;

4.8.1.2.3. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk, in accordance with applicable agency and OIT policies and procedures.

5.0. Document Information

5.1. Initial Issue Date: August 30, 2019
5.2. Latest Revision Date: May 21, 2021
5.3. Point of Contact: Enterprise.Architect@Maine.Gov
5.4. Approved By: Chief Information Officer, OIT
5.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[3]
5.6. Waiver Process: Waiver Policy[4]
5.7. Distribution: Internet[5]

6.0. Review

This document is reviewed annually and when substantive changes are made to policies, procedures, or other authoritative regulations that affect it.

7.0. 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 3 years and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these

[2] https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf
[3] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/waiver.pdf
[5] https://www.maine.gov/oit/policies-standards

documents will be subject to any future State Archives General Schedule revisions that cover these categories.

8.0. Public Records Exceptions

Under the Maine Freedom of Access Act (FOAA), 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.

9.0. Definitions

9.1. Information asset: Used interchangeably with information system. A discrete, identifiable piece of information technology, including hardware, software, and firmware. Information assets include, for example, mainframes, workstations, servers (including database, electronic mail, authentication, web, proxy, file, and domain name), input/output devices (such as scanners, copiers, printers), network components (firewalls, routers, gateways, voice and data switches, process controllers, wireless access points, network appliances, and sensors), operating systems, virtual machines, middleware, business applications, system software, development tools, and miscellaneous related utilities.

9.2. 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.

10.0. Abbreviations

10.1. FOAA: (Maine) Freedom of Access Act.
10.2. OIT: Office of Information Technology.
10.3. SOM: State of Maine.
10.4. VPN: virtual private network.