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 (see Definitions) 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 Executive Branch managed services.

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. Any State of Maine personnel that accesses a State of Maine information asset must have an Active Directory account in their respective branch's (Executive, Judicial, Legislative, etc.) directory.

4.2.2. 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.

4.2.2.1. OIT uses the following types of authorized user (see Definitions) accounts:

4.2.2.1.1. Individual accounts;
4.2.2.1.2. Role-based shared accounts;
4.2.2.1.3. Group accounts; and
4.2.2.1.4. System accounts.

4.2.3. Agencies must assign gatekeepers to manage agency information asset account authorizations.

4.2.3.1. OIT utilizes the Enterprise Ticketing System to manage user account requests (establish, modify, or terminate user access accounts).

4.2.3.2. Authorized agency personnel submit user account requests via the Enterprise Ticketing System user request web form, providing all required information and justification for the request.

4.2.3.2.1. 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.

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

4.2.4. 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;

4.2.4.1. Authorized agency personnel provide approval and specify this information in the Enterprise Ticketing System ticket user access request to OIT.

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

4.2.4.2.1. Authorizing access to the information asset based on:

4.2.4.2.1.1. A valid access authorization;

4.2.4.2.1.2. Intended system usage; and

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

4.2.4.3. Agencies must monitor the use of agency information asset accounts and notify OIT through the Enterprise Ticketing System when:

4.2.4.3.1. Accounts are no longer required;

4.2.4.3.2. Personnel are terminated or transferred; and

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

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

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

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.

4.2.8. All printers used to conduct State of Maine business must only connect to the State network via a wired connection, Ethernet and USB are both allowable.

4.2.9. For Active Directory user accounts, no service is allowed for the creation or updating of the primary key-attributes. Some secondary key-attributes may be open for self-service updating.

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 Enterprise 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 Enterprise Ticketing System 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, 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 the authorized access necessary to accomplish assigned tasks, in accordance with job duties and 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. **Inbound and Outbound Wide Area Network Remote Access**

4.6.1. Any inbound Remote Access VPN to the State of Maine Wide Area Network must be via the Cisco AnyConnect application installed on the individual device.

4.6.2. In rare cases, the CISO may approved State-owned or managed devices to connect to a partner's corporate network for business reasons, requiring installation of the partner's VPN application. The Information Security Office will maintain an authorized list of approved VPN applications and track associated devices and use cases.

4.7. Irrespective of anything else, under no circumstance is a device owned and/or managed by the State of Maine allowed to initiate a dual-VPN split-tunnel, i.e., a simultaneous VPN connection to both the State of Maine Wide Area Network and a remote partner's corporate network.

4.8. **In-State Remote Access (AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4))**

4.8.1. Both the agencies and OIT must ensure that usage restrictions, configuration and connection requirements, and implementation guidance for In-State Remote Access (see Definitions) 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.

4.8.1.1. OIT requires that In-State Remote Access occurs via established virtual private networks (VPNs) utilizing multifactor authentication and host verification (host operating system checker and anti-malware).

4.8.1.2. Secure tokens, assigned to specific individuals, are required for In-State Remote Access. These secure tokens are issued by OIT upon receipt of a request from authorized agency personnel.

4.8.1.3. 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.

4.8.1.4. OIT monitors and controls In-State Remote Access, using a secure portal with automated, standard reporting capabilities.

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

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

4.8.1.6. OIT utilizes two distinct, dedicated domain entry points to route all In-State Remote Access.

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

4.8.1.7.1. Given that authorization is role-based, the user has the same privileges, regardless of whether In-State Remote Access or on-premises.

4.8.1.7.2. Authorized access is documented.

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

4.8.1.8.1. Up-to-date system patches;

4.8.1.8.2. Current anti-malware; and

4.8.1.8.3. Automatic code execution disabled.

4.9. Short-Term Out-of-State Domestic Remote Access (AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4))

4.9.1. Personnel intending Short-Term (see Definitions) Out-of-State Domestic Remote Access (see Definitions) must make a request to their supervisor.

4.9.2. The supervisor must acknowledge, and either approve or deny the applicant personnel's request. Should the supervisor deny the request, no further action is necessary.

4.9.3. Should the supervisor approve the request and should the applicant personnel happen to be a State Employee (as opposed to a Contractor), the supervisor ensures compliance with the agency's out-of-state travel approval workflow. Should the agency approve such out-of-state travel, then the State Employee proceeds with the Short-Term Out-of-State Domestic Remote Access.

4.9.4. For Contractors, the Short-Term Out-of-State Domestic Remote Access is *not* subject to approval by the DAFS Bureau of Human Resources.

4.9.5. Otherwise, the Short-Term Out-of-State Domestic Remote Access follows the same procedure as In-State Remote Access (see 4.6, above).

4.10. Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access (irrespective of Long or Short-Term) (AC-17, AC-17(1), AC-17(2), AC-17(3), AC-17(4))

4.10.1. Any data that is subject to Federal compliance mandates (including, but not limited to Criminal Justice Information Systems (CJIS), Internal Revenue Service (IRS), and Centers for Medicare and Medicaid Services (CMS)) must never be subjected to Foreign Remote Access.

4.10.2. Compared to In-State Remote Access and Short-Term Out-Of-State Domestic Remote Access, Long-Term Out-of-State Domestic Remote Access (see Definitions) and Foreign Remote Access (see Definitions) demand additional review, and the related workflow is described below. Unless explicitly called out in this section, all other details follow the In-State Remote Access described in section 4.6.

4.10.3. The State of Maine must ensure that Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access to agency information assets is explicitly authorized prior to allowing such access, and is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.10.3.1. Personnel intending Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access to State information must make a request to their supervisor.

4.10.3.2. The supervisor must acknowledge, and either approve or deny the applicant personnel's request. Should the supervisor deny the request, no further action is necessary. Supervisors must exercise great caution before approving Foreign Remote Access. Foreign Remote Access is fraught with numerous variables that make risk determination challenging. Such variables include, but are not limited to, foreign relations, international terrorism, international law, crime statistics at that locale, etc. Some general guidance may be found from the U.S. State Department Travel Advisories.[1]

4.10.3.3. Should the supervisor approve of the Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access request of the applicant personnel, then, only for State Employees, the supervisor submits an approval request to the DAFS Bureau of Human Resources. This step is *not* necessary for Contractors. For State Employees, should the DAFS Bureau of Human Resources deny the request, no further action is necessary.

4.10.3.4. Should, for State Employees, the DAFS Bureau of Human Resources approves the Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access, the supervisor submits a request, through the OIT Enterprise Ticketing System, no later than 10 business days prior to the commencement of the requested Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access. (The OIT Enterprise Ticketing System service is called "Application for Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access".) At a minimum, such a request must include:

4.10.3.4.1. Name (as listed in the Active Directory), and Maine.Gov directory email address, of the applicant personnel;

4.10.3.4.2. The Title and the Job Responsibilities of the applicant personnel;

[1] https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

4.10.3.4.3. The full list of information assets the applicant personnel will access, and the data classification of such assets. (See the Data Classification Policy[2] for more details);

4.10.3.4.4. The projected timeline of the Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access request (see definitions of Long-Term and Short-Term);

4.10.3.4.5. The device(s) that would be used for the Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access, including whether said devices are managed by the Office of Information Technology;

4.10.3.4.6. Whether the accessing location is going to be stationary for the stated time, or not. If not, the complete list of locations and times of such access must be provided; and

4.10.3.4.7. Either an explicit statement, or evidence, of the supervisor's approval of this Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access request; and

4.10.3.4.8. A copy of the approval from the DAFS Bureau of Human Resources for State Employees.

4.10.3.5. This Enterprise Ticketing System request is assigned to OIT Security.

4.10.3.6. OIT Security:

4.10.3.6.1. Conducts a risk assessment of the destination;

4.10.3.6.2. Provides a recommendation to the Chief Information Security Officer (CISO), who either approves or denies the request. Denied requests are provided to the Chief Information Officer (CIO) for a final determination; and

4.10.3.6.3. If approved by the CISO/CIO, the ticket is handed off to other Office of Information Technology service verticals for operational implementation.

4.10.3.7. In the case of approved Long-Term Out-of-State Domestic Remote Access, the applicant personnel will continue using their regular work laptop.

4.10.3.8. In the case of approved Foreign Remote Access, the following will be executed:

4.10.3.8.1. The applicant personnel is provisioned with a basic laptop, and multi-factor authentication, for travel;

4.10.3.8.2. This basic laptop is *only* utilized to connect to the second virtual workstation described below. No actual State work is performed on the basic laptop. No State data is ever stored on the basic laptop; and

4.10.3.8.3. The applicant personnel is also provisioned with a second virtual workstation inside the State wide area network. All actual work is performed on this workstation.

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

4.10.3.9. Irrespective of the supervisor's approval, depending upon the assessed risk to State information assets from the requested Long-Term Out-of-State Domestic Remote Access or Foreign Remote Access, OIT retains the right to deny the request at any point in the future.

4.10.3.10. TLP: Amber and TLP: Red data cannot be accessed by agency personnel located in foreign countries, with the exception of U.S. territories, embassies, and military installations. Further, TLP: Amber and TLP: Red data may not be received, processed, stored, transmitted, or disposed of by information assets located overseas (See the Data Classification Policy[3] for more details).

4.11. Disconnect/Disable Remote Access (AC-17(9))

4.11.1. OIT, with support from the agencies, must have the ability to expeditiously disconnect users remotely accessing agency information systems and/or disable future remote access in order to secure agency information assets. In addition to the below, see also 5.1.3. of Network Device Management Policy[4].

4.11.1.1. The CIO, CISO, Networking, CIS, or Client Tech management is authorized to order:

4.11.1.1.1. The immediate disconnection of remote network connections, and/or

4.11.1.1.2. The immediate disabling of future remote network access.

4.11.1.2. After the order is received, the connection(s) should be terminated and the disabling of future remote connection(s) should be completed promptly, preferably within 15 minutes.

4.11.1.3. Networking, CIS, or Client Tech management will notify the CISO of the actions taken.

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

4.12.1. 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.

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

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

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

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

4.12.1.1.2. SOM GUEST: 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 (see Definitions). User audits identifying "permanent type" connections on SOM GUEST can lead to charges of network access rates to the agency.

4.12.1.2. OIT strictly prohibits the installation of wireless access points that are not managed by OIT.

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

4.12.1.3.1. Encryption protection is enabled;

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

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

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

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

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

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

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

4.12.1.4.3. Static IP addresses are not used for client devices; instead, Dynamic Host Configuration Protocol (DHCP) is utilized; and

4.12.1.4.4. 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.

4.12.1.5. Wireless access is protected using authentication and encryption.

4.12.1.6. OIT uses 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.

4.12.1.7. See System and Information Integrity Policy,[5] Information System Monitoring (SI-4) for more details.

4.12.1.8. All printers used to conduct State of Maine business must only connect to the State network via a wired connection, Ethernet and USB are both allowable.

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

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

4.13.1. 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 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.

4.13.1.1. The OIT Mobile Device Policy[6] establishes the requirements for mobile device access to the State network. These requirements include, but are not limited to:

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

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

4.13.1.1.3. Mobile device management software requirements.

4.13.1.2. Additionally, OIT:

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

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

4.13.1.2.3. 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.

4.13.2. All printers used to conduct State of Maine business must only connect to the State network via a wired connection, Ethernet and USB are both allowable.

5.0. Document Information

5.1. Initial Issue Date: August 30, 2019

5.2. Latest Revision Date: December 11, 2024

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[7]

5.6. Waiver Process: Waiver Policy[8]

5.7. Distribution: Internet[9]

6.0. Review

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

[6] https://www.maine.gov/oit/policies/MobileDevicePolicy.pdf

[7] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

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

[9] https://www.maine.gov/oit/policies-standardss

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 a minimum of 6 years after withdrawal or replacement and then destroyed in accordance with guidance[10] provided by Maine State Archives. Retention of these 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),[11] 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.

9.0. Definitions

9.1. 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).

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

9.3. 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.

9.4. 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.

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

9.6. Long-term: 30 days or more.

[10] https://www.maine.gov/sos/arc/records/state/GS1Administrative.pdf

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

9.7. 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.

9.8. Personal devices: Include the following categories:

9.8.1. 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);

9.8.2. 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

9.8.3. 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.

9.9. 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.

9.10. Remote Access VPN: A Remote Access VPN is different from a Site-to-Site (S2S) VPN (See https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SiteToSiteVPNPolicy.pdf for more info). An S2S VPN connects two different corporate networks through an encrypted tunnel. Whereas, a Remote Access VPN connects an individual device to a corporate network through an encrypted tunnel. Establishing a Remote Access VPN involves installing a native operating system application on the individual device which forms one endpoint of the encrypted tunnel; The other endpoint being the remote corporate network. From the standpoint of a corporate network, a Remote Access VPN can be either Inbound, or Outbound. An Inbound Remote Access VPN connects a foreign device into the corporate network. Whereas, an Outbound Remote Access Network connects a device within the corporate network into a remote partner's corporate network.

9.11. Short-term: Fewer than 30 days.

10.0. Abbreviations

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