State of Maine
Department of Administrative and Financial Services
Office of Information Technology (OIT)

Physical and Environmental Protection Policy and Procedures (PE-1)

Table of Contents

1.0. Purpose

This policy establishes the State of Maine's information technology physical and environmental protection. This corresponds to the Physical and Environmental Protection (PE) Control Family, of the National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4).

2.0. Scope

2.1. This document applies to:

2.1.1. All State of Maine Office of Information Technology employees and contractors (collectively referred to as personnel in this document);

2.1.2. Only the two OIT data centers and the OIT Headquarters.

3.0. Conflict

If this document 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. OIT Information Security

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

4.1.2. Ensures all OIT personnel are aware of all applicable penalties for non-compliance;

4.1.3. Oversees and facilitates badging processes;

4.1.4. Facilitates the biannual review process for OIT personnel;

4.1.5. Recalls access control and visitor logs as needed for causative research;

4.1.6. Maintains the Authorized Access List for personnel to the OIT Headquarters through the Honeywell system; and

4.1.7. Maintains access control log reports of personnel with authorized access for review as necessary.

4.2. OIT Facilities Manager (Within the Network Operations Team)

4.2.1. Coordinates maintenance operations, including addressing problems/issues that have been reported;

4.2.2. Secures network access through such entry points including, but not limited to, network jacks, network cabling, and other remote infrastructure.

4.2.3. Passes along statuses and information to Department of Administrative and Financial Services (DAFS) Property Management;

4.2.4. Oversees the physical facilities (OIT Headquarters and data centers) including site planning, equipment security, environmental controls, coordination of new construction, and installation of equipment;

4.2.5. Reviews the visitor log for data centers; and

4.2.6. Maintains the Authorized Access List for personnel to the data centers through the Honeywell system.

4.3. Securitas (Uniformed Security)

4.3.1. Manages the visitor badge process and monitors all access to the OIT Headquarters; and

4.3.2. Conducts foot patrols in and around the OIT Headquarters on a routine basis.

4.4. Server Support Staff (of Computing Infrastructure and Services and Enterprise Data Services)
4.4.1. Authorize, monitor, and control any server hardware entering and exiting the data centers.

4.5. OIT Client Technologies
4.5.1. Oversees delivery and removal of user equipment within the OIT Headquarters.

4.6. OIT Personnel
4.6.1. Comply with this Policy and Procedures;
4.6.2. Report missing, misplaced, stolen, and/or damaged access cards; and
4.6.3. Secure their access cards against unauthorized use.
4.6.4. Display their access cards below their shoulders and above their waist.

4.7. Bureau of General Services (BGS)
4.7.1. Works with OIT Information Security, the OIT Facilities Manager, and the OIT Network Operations Team to coordinate the physical security of State of Maine Information assets.

4.8. Agency Business Partners
4.8.1. Ensure all personnel understand that they are responsible for the physical security of all State of Maine information assets entrusted in their care (i.e., given to them).

5.0. Management Commitment

The State of Maine is committed to following this document.

6.0. Coordination Among Agency Entities

The Office of Information Technology coordinates physical security through BGS to ensure the security of State of Maine information assets (see Definitions) in accordance with Executive Order 2014-003[1] and Title 5, Chapter 163 §1971-1985.[2] Agencies and OIT coordinate to meet all state and federal audit documentation and reporting compliance requirements.

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 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.

[1] http://www.maine.gov/tools/whatsnew/attach.php?id=626944&an=1
[2] https://legislature.maine.gov/statutes/5/title5ch163sec0.html

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

8.1. The procedures listed below in this section are designed to satisfy the security control requirements of this policy (PE-1) as outlined in Internal Revenue Service (IRS) Publication 1075, and to satisfy federal law.

8.2. Physical Access Authorizations (PE-2)

8.2.1. Within OIT data centers, OIT Information Security works with BGS to:

8.2.1.1. Issue authentication credentials (e.g., badges, identification cards, and smart cards) to everyone authorized to access a restricted area.

8.2.1.1.1. Everyone within an OIT data center or the OIT Headquarters building must clearly display either a State identification badge or a current and numbered visitor badge above the waist. These badges are the property of the State and are provided to employees and visitors as a convenience. Badges must always be visible.

8.2.1.1.2. Keys, combinations, and other physical access devices are always secured to prevent unauthorized access to agency facilities and assets.

8.2.1.1.3. Personnel must question anyone attempting to gain access to secure areas through tailgating / piggybacking—attempting to gain access by closely following someone who has authorized access. Personnel must notify Uniformed Security personnel and OIT Information Security of any such attempt.

8.2.1.2. Develop, approve, and maintain a list of individuals with authorized access to the facility.

8.2.1.3. Review the access list detailing authorized facility access by individuals semi-annually.

8.2.1.3.1. The Security Event and Incident Manager, managed by the Information Security Office, is used to facilitate the semi-annual access review.

8.2.1.4. Generate emails to supervisors to confirm the current list of direct reports with active badges.

8.2.1.5. Remove individuals from the facility access list when access is no longer required.

8.2.1.6. **Access by Position/Role (PE-2(1)):** Authorize physical access to the facilities based on position or role.

8.2.1.7. Utilize a standard operating procedure to manage access when onboarding a new employee.

8.2.1.7.1. The supervisor submits a ticket through the Enterprise

Ticketing System (or by email[3]) for a new badge (see Personnel Security Policy and Procedures, PS-1[4]), detailing who and what kind of access the employee will need following the principle of least privilege (see Definitions).

8.2.1.7.2. Badge issuance is subject to a standard approval workflow.

8.2.2. Within OIT Headquarters, OIT Information Security works with BGS to:

8.2.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.3. Physical Access Controls (PE-3)

8.3.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.3.1.1. Enforce physical access authorizations at the main entry point to the two OIT data centers by:

8.3.1.1.1. Verifying individual access authorizations through a badge reader or upon presentation of a government issued ID before granting access to the facility;

8.3.1.1.2. Controlling ingress/egress to the facility using cameras, electronic access controls (see Definitions), and other physical hardening devices;

8.3.1.1.3. Maintaining physical access audit logs for any area secured by a badge reader;

8.3.1.1.3.1. Logs are reviewed by OIT Information Security on request and whenever there is an incident.

8.3.1.1.3.2. Access logs for those with approved access are provided by BGS to OIT Information Security on request with approval from Human Resources.

8.3.1.1.3.3. The manual visitor logs for the OIT data centers and OIT Headquarters are maintained by the OIT Facilities Manager and Securitas respectively.

8.3.1.1.4. Providing cameras, electronic access control, and other physical hardening devices to control access to areas within the facility officially designated as publicly accessible;

8.3.1.1.5. Securing keys and other physical access devices;

8.3.1.1.6. Inventorying badges every six months;

8.3.1.1.7. Managing changes in keys as needed and/or when keys

[3] OIT.Customer-Support@maine.gov

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

are lost, compromised, or individuals are transferred or terminated;

8.3.1.1.8. Requiring all visitors to be escorted by the employee they are visiting and be monitored by the employee while on premises;

8.3.1.1.9. Reviewing visitor logs monthly; and

8.3.1.1.10. Enforcing physical access authorizations to the information system in addition to the physical access controls for the facility at each entry to the data center and internal spaces.

8.3.1.2. Temporarily issued physical access keys are issued by Building Access Control (BAC) and assigned to individuals using the Key Conductor system. Permanently assigned keys are managed by OIT and assigned to individuals.

8.3.1.3. The inventory, maintenance, and monitoring of other physical security devices besides badges and keys (e.g., badge readers, cameras) is handled by BGS. Security and Maintenance operates the BAC that provides safety, security, and efficiency by operating a complex integrated building management system for all State-owned and leased facilities statewide, which includes all associated parking areas.

8.3.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.3.2.1. Require all visitors entering the lobby to sign in with security to be assigned a temporary badge;

8.3.2.2. In addition to the controls outlined in 8.3.1, control access with security guards.

8.3.2.3. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.3.3. Badge photos must be renewed, with a current photo, at least once every five years.

8.4. **Access Control for Transmission Medium (PE-4)**

8.4.1. Within OIT data centers, OIT Information Security works with BGS, the OIT Facilities Manager, and the rest of Network Operations to:

8.4.1.1. Control physical access to information system distribution and transmission lines by:

8.4.1.1.1. Using badge access and Active Directory accounts;

8.4.1.1.2. Locking wiring closets;

8.4.1.1.3. Disconnecting or locking spare network jacks; and

8.4.1.1.4. Protecting cabling by conduit or cable trays.

8.4.1.2. Guarantee publicly accessible network jacks in data centers provide only Internet access by default, unless additional functionality is

explicitly authorized.

8.4.1.3. Restrict physical access to networking equipment and cabling to authorized personnel.

8.4.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.4.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.5. **Access Control for Output Devices (PE-5)**

8.5.1. Within OIT Headquarters and OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

8.6. **Monitoring Physical Access (PE-6)**

8.6.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.6.1.1. **Intrusion Alarms/Surveillance Equipment (PE-6(1)):** Monitor physical access to the two OIT data centers where information systems reside to detect physical intrusion alarms and surveillance equipment and respond to physical security incidents;

8.6.1.2. Review physical access logs upon occurrence of any incident that would warrant investigation of the physical access logs; and

8.6.1.3. Coordinate results of reviews and investigations with the incident response team.

8.6.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.6.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.7. **Visitor Access Records (PE-8)**

8.7.1. Within OIT data centers and OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.7.1.1. Retain visitor access logs for at least five years;

8.7.1.2. Review headquarters visitor access logs as needed; and

8.7.1.3. Review data center visitor access logs at least monthly.

8.8. **Power Equipment and Cabling (PE-9)**

8.8.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.8.1.1. Protect both power and communication lines;

8.8.1.2. Employ backup power generation equipment; and

8.8.1.3. Employ automatic voltage controls for critical system components to help ensure that power continues to flow in the event voltage fluctuates to unacceptable levels to avoid damage to the information system component.

8.8.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.8.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.9. **Emergency Shutoff (PE-10)**

8.9.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.9.1.1. Provide the capability of shutting off power to information systems or individual system components in emergency situations.

8.9.1.2. Provide each cabinet with the ability to shut off power on an as-needed basis.

8.9.1.3. Protect emergency power shutoff capability from unauthorized activation by badge entry.

8.9.1.4. Protect the emergency power-off capability from accidental or unauthorized activation. The Uptime Institute® notes that 70% of outages at data center facilities are caused by human error. Considering this fact, one of the goals of the design was to minimize the existence of elements such as Emergency Power Off (EPO) pushbuttons, which could lead to unplanned outages due to human error.

8.9.1.5. The Sewall Street Data Center does not have an EPO per Article 90 of the National Electrical Code, Paragraph 645.4, Special Requirements for Information Technology Equipment Room (see the OIT Facilities Manager for further details).

8.9.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.9.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.10. **Emergency Power (PE-11)**

8.10.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.10.1.1. Provide short-term uninterruptible power supply (UPS) (see Definitions) to facilitate an orderly shutdown of the information system and transition the information system to a long-term alternate power in the event of a primary power source loss.

8.10.1.2. Employ use of a UPS to avoid abnormal shutdowns or to provide a

clean power source during brownouts or surges.

8.10.1.3. Employ contingency plans that include procedures to follow if the UPS fails (see Information Systems Contingency Plan,[5] intranet only).

8.10.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.10.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.11. **Emergency Lighting (PE-12)**

8.11.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.11.1.1. Employ and maintain automatic emergency lighting for information systems that activate in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the OIT data centers. The automatic emergency lighting is backed up by a generator.

8.11.1.2. Test the automatic emergency lighting systems annually to ensure they are fully operational.

8.11.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.11.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.12. **Fire Protection (PE-13)**

8.12.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.12.1.1. Employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source using a heavy gas, 3M Novec (see Definitions), and/or water.

8.12.1.1.1. **Automatic Fire Suppression (PE-13(3)):** All fire suppression and detection systems are automated.

8.12.2. **Detection Devices/Systems (PE-13(1)):** Employ smoke/fire detection devices that activate automatically and notify the BCC in the event of a fire.

8.12.3. **Suppression Devices/Systems (PE-13(2)):** Employ water as a fire suppression device that provides automatic notification of any activation to the BCC.

[5] http://inet.state.me.us/oit/policies/documents/InformationSystemsContingencyPlan.pdf

8.12.4. Within OIT Headquarters, OIT:
8.12.4.1. Has a National Fire Protection Association compliant alarm/suppression system.

8.13. **Temperature and Humidity Controls (PE-14)**
8.13.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:
8.13.1.1. Maintain temperature and humidity levels within vendor-recommended levels.
8.13.1.1.1. BGS monitors temperature and humidity levels daily to ensure they remain within vendor-recommended levels. BGS alerts the OIT Facilities Manager of alarms.
8.13.1.1.2. The heating, ventilation, and air conditioning (HVAC) vendor is on standby to address issues as they arise.

8.13.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:
8.13.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

8.14. **Water Damage Protection (PE-15)**
8.14.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:
8.14.1.1. Protect against water damage due to flood or leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel;
8.14.1.2. Use a raised floor to protect from flooding; and
8.14.1.3. Use water sensors to detect potential flooding or leakage which will trigger a shutoff.

8.14.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:
8.14.2.1. Reports issues to DAFS Property Management to be addressed.

8.15. **Delivery and Removal (PE-16)**
8.15.1. Within OIT data centers, OIT Information Security works with BGS, OIT Facilities Manager, the Network Operations Team, and the server support staff to:
8.15.1.1. Authorize, monitor, and control any hardware entering and exiting the facility. Records of these items are maintained within the Enterprise Ticketing System and can be audited by supervisors and the Change Advisory Board (CAB).

8.15.2. Within OIT Headquarters, OIT Information Security works with BGS, Client Technologies, and the OIT Facilities Manager to:

8.15.2.1. Track equipment that has been deployed to users using the Enterprise Ticketing System, Active Directory, and the inventory system.

8.15.2.1.1. OIT Client Technologies delivers equipment to personnel.

8.15.2.1.2. OIT tracks what equipment has been deployed to which user to ensure that equipment is returned when an employee leaves State service.

8.15.2.1.3. When users wish to return equipment, a request is initiated through the Enterprise Ticketing System to return equipment or have equipment picked up. Once received, the Enterprise Ticketing System and the inventory management system are updated to note that the device and appropriate accessories have been returned.

8.15.3. All personnel are responsible for the physical security of all State of Maine information assets entrusted in their care (i.e., given to them).

8.16. Alternate Work Site (PE-17)

8.16.1. For both remote and on-site work, the following security controls are employed:

8.16.1.1. Personnel exclusively work using State of Maine devices;

8.16.1.2. The Rules of Behavior apply;[6]

8.16.1.3. Employees communicate and report security incidents in accordance with the Cyber Incident Reporting Procedures (intranet only);[7]

8.16.1.4. The network is monitored continuously.

8.16.2. When employees work remotely, the following security controls are employed:

8.16.2.1. Remote access occurs in accordance with AC-17, Remote Access (see Access Control Procedures for Users)[8] and Identification and Authentication Policy and Procedures (intranet only),[9] using virtual private networks, multi-factor authentication, and host verification.

[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/rules-of-behavior.pdf
[7] http://inet.state.me.us/oit/policies/documents/IncidentReportingProcedures.pdf
[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/access-control-procedures-for-users.pdf
[9] http://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf

8.17. **Location of Information System Components (PE-18)**

8.17.1. Within OIT data centers, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.17.1.1. Protect information system components as detailed in PE-9 to PE-15 above.

8.17.1.2. Ensure the safety of the physical space.

8.17.1.2.1. BGS requires architect and engineer consultants to design all spaces to meet applicable building codes which protect the health, safety, and welfare of those who utilize the spaces. Specific requirements for particular spaces may be provided by agencies in order to meet their mission.

8.17.1.2.2. Consultants are responsible for identifying all applicable codes and ordinances and applying them to the design of the project. The State of Maine has a central agency (the Bureau of Building Codes in the Office of State Fire Marshal)[10] for managing various code requirements, and codes are administered at a local level by Code Enforcement Officers and Fire Chiefs.

8.17.2. Within OIT Headquarters, OIT Information Security works with BGS and the OIT Facilities Manager to:

8.17.2.1. Meet the intended outcome for these controls using methods that are adapted for an office space setting versus a data center environment.

9.0. Document Details

9.1. Initial Issue Date: August 31, 2021
9.2. Latest Revision Date: December 2, 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[11]
9.6. Waiver Process: Waiver Policy[12]
9.7. Distribution: Internet[13]

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

Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and*

[10] https://www.maine.gov/dps/fmo/building-codes
[11] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[12] https://www.maine.gov/oit/policies/waiver.pdf
[13] https://www.maine.gov/oit/policies-standards

Directives records management categories. They will be retained for three years, and then destroyed in accordance with guidance 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), 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.

13.0. Definitions:

13.1. 3M Novec: A clean agent fire extinguishant which was developed as a halon replacement and hydrofluorocarbon.

13.2. Electronic access controls: The technology used to provide and deny physical or virtual access to a physical or virtual space. That space can be, for example, the building itself, or an executive suite.

13.3. Information Asset: Used interchangeably with Information System. 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).

13.4. Principle of least privilege: The philosophy of providing the least amount of access to secure resources to allow maximum control over protection of resource.

13.5. Uninterruptible Power Supply (UPS): An electrical apparatus that provides emergency power to a load when the input power source or main power fails.

14.0. Abbreviations

14.1. BAC: Building Access Control
14.2. BGS: Bureau of General Services
14.3. CAB: Change Advisory Board
14.4. FOAA: (Maine) Freedom of Access Act
14.5. HVAC: Heating, Ventilation, and Air Conditioning
14.6. IRS: Internal Revenue Service
14.7. NIST: National Institute of Standards and Technology
14.8. OIT: Office of Information Technology
14.9. UPS: Uninterruptible Power Supply