



Division of Information Technology

Enterprise Technology Strategy and Services Policy 10-16

Physical and Environmental Security Policy

Last Revision: 11/8/2022

Brian Tardiff, CISO

doa.entsec@doit.ri.gov

1. Purpose

Establish policy for the implementation of adequate physical and environmental security controls at data centers and facilities where data centers reside to ensure the protection of information systems and supporting components and infrastructure from physical and environmental hazards.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments¹ (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "Agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

Authorized Access List (AAL)

A list of personnel (e.g. employees, contractors, vendors) granted authorization credentials to access non-public areas of a facility where an information system resides.

Authorization Credentials

A method of identification used by personnel to access an information system facility. Identification methods include, for instance, badges, identification cards, and smart cards.

Data Center

A facility that houses information systems, network components, telecommunications, and other equipment. Data centers may also include redundant network connections, backup power supplies, and other systems necessary for proper maintenance and ongoing operations, such as environmental controls. Data centers may be any size, both large and small, and are sometimes referred to as computer rooms.

¹ State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)

Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)

Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. [IAL1, IAL2] Physical and Environmental Policy and Procedures (PE-1). The agency will develop, document, disseminate to designated personnel defined in the applicable system security plan, review, and annually update a physical and environmental policy and procedures.

4.2. [IAL1, IAL2] Physical Access Authorizations (PE-2). The agency will:

1. Develop, approve, and maintain an AAL of individuals authorized to access the facility where the information system resides (areas not publicly accessible). Physical access to confidential or sensitive data, including PII, will be controlled (e.g. restricted areas, security rooms, locked rooms).
2. Issue authorization credentials for access to non-public areas of the facility. ID badge access cards will adhere to [DCAMM State Identification/Access Card Policy](#).
3. Review the AAL no less than:
 - a. Annually, for state employees.
 - b. Quarterly, for vendors and contractors.
4. Promptly remove individuals from the AAL when access is no longer required.

4.3. [IAL1, IAL2] Physical Access Control (PE-3). The agency will:

1. Identify public and non-public areas of the facility. Signs will be posted designating areas that have restricted physical access and are not publicly accessible. There will be no signs indicating that an information system, computer room, or data center is located within a particular area of the facility, nor will the information system be visible to a casual observer from outside the facility.
2. Implement appropriate safeguards (e.g. cameras, security guards, door/window locks) to monitor and control access to non-public areas of the facility. Two barriers will be

Division of Information Technology

implemented to protect access to PII under normal security (e.g. secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container).

3. Enforce physical access authorizations to controlled non-public areas of the facility by:
 - a. Verifying each access authorization prior to granting access to the facility.
 - b. Controlling facility entry and exits points using an access control system, device, or security guard. Only authorized personnel are allowed access to controlled non-public areas.
4. Maintain physical access audit logs of individuals accessing controlled non-public areas of the facility.
5. Escort and monitor the activity of visitors (e.g. vendors, contractors, maintenance, and facilities personnel) not authorized to access controlled non-public areas of the facility. Visitors will be escorted at all times by appropriate agency personnel within controlled non-public areas of the facility. Only authorized personnel granted an ID-badge with appropriate permissions to access controlled non-public areas of the facility are authorized unescorted access.
6. Secure keys, combinations to locks, and other physical access devices from unauthorized access.
7. Perform an annual inventory of all physical access devices, including cipher locks, keys, keycards, and card readers.
8. Change cipher lock combination codes annually, after an actual or suspected compromise of the code, when there is a theft or security violation within the controlled area being protected by the code, or an employee with knowledge of the code is transferred, terminated, or no longer requires access to the controlled area secured by the code.
9. Change key/keycard when the key/keycard is reported as being lost or stolen, when there is a theft or security violation within the controlled area being protected by the key/keycard, or an employee having the key/keycard is transferred, terminated, or no longer requires access to the controlled area secured by the key/keycard. A keycard is any card that grants access to a restricted area but does not uniquely identify the holder of the keycard (an employee ID badge is not a keycard).
10. Maintain a list of personnel issued cipher lock combination codes, keys, or keycards. Personnel will promptly return assigned keys and key cards to the agency upon or prior to separation, transfer, or termination from the agency.

4.4. [IAL2] Access Control for Transmission (PE-4). The agency will control physical access for information system and system component transmission and distribution lines to authorized personnel only to help prevent accidental damage, disruption, physical tampering, and eavesdropping of unencrypted transmissions. Wiring closets will be locked and unused physical ports (within wiring closets and patch panels) will be disabled.

4.5. [IAL2] Access Control for Output Devices (PE-5). The agency will protect and control access to information system output devices, including monitors, printers, copiers, and fax machines, to prevent unauthorized individuals from obtaining the output. Output

Division of Information Technology

devices should be located within secured areas that can only be accessed by authorized individuals and monitored by agency personnel. Where required to meet federal or state law or program compliance requirements, the agency should implement keypad or card reader access controls for access to output devices.

4.6. [IAL1, IAL2] Monitoring Physical Access (PE-6). The agency will:

1. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.
2. Review physical access logs no less than monthly for suspicious activity, including access that is outside of normal work hours, repeated access to areas not normally accessed, access that lasts for unusual lengths of time, and access that is out-of-sequence.
3. Coordinate results of reviews with ETSS and agency incident response capability.

4.6.1. [IAL2] Intrusion Alarms and Surveillance Equipment (PE-6.1). The agency will:

1. Monitor and secure the facility where the information system resides with physical intrusion alarms and surveillance equipment.
2. Perform quarterly reviews of physical intrusion alarms and surveillance equipment for effectiveness during both normal business hours and when facilities are unoccupied.

4.7. [IAL1, IAL2] Visitor Access Records (PE-8). The agency will:

1. Maintain visitor access records to the facility where the information system resides in accordance with State of Rhode Island General Records Retention Schedule [GRS3.2](#), as required by federal or state law or regulatory compliance requirement, or for a minimum of one (1) year, whichever is longer. Visitor access records will include, at a minimum, the name and organization of visitors, visitor signatures (physical or electronic), form of identification provided, date of access, entry/departure times, purpose of visit, and name and organization of person visited. This control does not apply to access records for areas within the facility that are designated as publicly accessible.
2. Review visitor access records no less than monthly.
3. Report anomalies in visitor access records to the facilities manager or agency Technical Support Manager (TSM).

4.8. [IAL2] Power Equipment and Cabling (PE-9). The agency will protect power equipment and cabling (e.g. transmission and distribution lines) for the information system from damage and destruction, including generators and power cabling located outside the facility, internal cabling and uninterruptable power supplies (UPS) located inside the facility, and HVAC systems. Only authorized maintenance personnel are permitted to access this type of equipment.

4.9. [IAL2] Emergency Shutoff (PE-10). The agency will install an emergency shutoff switch that:

Division of Information Technology

1. Cuts power to the information system or individual system components in emergency situations.
2. Is located near an exit door in a safe location easily accessible by personnel.
3. Is protected from unauthorized or inadvertent activation (e.g. clear plastic cover).

4.10. [IAL2] Emergency Power (PE-11). The agency will install an uninterruptible power supply (UPS) to facilitate an orderly information system shutdown or for the transition to an alternate power source in the event of a primary power loss. UPS maintenance activities will be performed in accordance with the manufacturer's recommended maintenance schedule to maximize the life of the UPS and ensure adequate backup power is available when needed in accordance with business continuity requirements.

4.11. [IAL1, IAL2] Emergency Lighting (PE-12). The agency will install and maintain emergency lighting for emergency exits and evacuation routes that automatically activates in the event of a power outage or disruption.

4.12. [IAL1, IAL2] Fire Protection (PE-13). The agency will install, maintain, and periodically test a fire suppression system and detection devices for the information system. Fire suppression systems should use an environmentally friendly gas whenever possible (water sprinkler systems are not an approved method of fire mitigation). See [National Fire Protection Association \(NFPA\)](#) for best business practices and standards.

4.12.1. [IAL2] Detection Systems - Automatic Activation and Notification (PE-13.1). The agency will install and maintain fire suppression systems that automatically activate and notify appropriate incident response and other designated personnel in the event of a fire.

4.13. [IAL1, IAL2] Environmental Controls (PE-14). The agency will:

1. Install temperature and humidity sensors in appropriate locations within the facility where the information system resides.
2. Monitor and maintains temperature and humidity levels daily in accordance with manufacturer recommendations (in general, approximately 70°F and 50% humidity).
3. Alert designated personnel when sensors detect temperature or humidity levels that are out of range. Designated personnel will report damage and provide remedial action, up to and including contingency plan activities, if necessary.

4.14. [IAL1, IAL2] Water Damage Protection (PE-15). The agency will

1. Protect the information system from water damage by installing a master shutoff and isolation zone valves (where appropriate) that are easily accessible.
2. Maintain master shutoff and isolation zone valves in proper operational condition.
3. Ensure key personnel know the location(s) of master shutoff and isolation zone valves.

4.15. [IAL1, IAL2] Delivery and Removal (PE-16). The agency will:

1. Authorize, monitor, and control information system components entering and exiting the facility. Effectively enforcing authorizations for entry and exit of information



Division of Information Technology

system components may require restricting access to delivery areas and isolating the areas from the information system and media libraries.

2. Maintain records of information system components entering and exiting the facility.

4.16. *[IAL2]* Alternate Work Site (PE-17). The agency will:

1. Identify and document alternate work sites allowed for use by employees.
2. Implement physical access controls at alternate work sites that provide similar safeguards and protections as primary worksites.
3. Annually assesses the effectiveness of controls at alternate work sites.
4. Provide a means for employees to communicate with information security and privacy personnel in the event of a security incident.

5. Approval / Review Signature

Chief Information Security Officer