Division of Enterprise Technology Strategy and Services

ETSS Policy 100.11

Physical and Environmental Security Policy (PE)

Publish Date: 23 June 2026

Effective Date: 23 June 2026

Last Review: 22 June 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for physical and environmental security controls at facilities that house State of Rhode Island information systems and support infrastructure. It provides a framework for protecting information systems and their components from physical threats, environmental hazards, and unauthorized physical access. This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Physical and Environmental Protection family), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements. By defining clear expectations for facility security, access management, environmental monitoring, and emergency preparedness, this policy helps safeguard the confidentiality, integrity, and availability of State data and critical technology infrastructure.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State. For the purposes of this policy, the term "Agency" refers to any department, agency, division, or unit of the Executive Branch.

This policy applies to all facilities where State information systems reside, including data centers, server rooms, wiring closets, and alternate work sites. It also applies to cloud and colocation environments where the State maintains shared responsibility for physical security controls, as documented in the applicable System Security Plan (SSP).

3. Roles and Responsibilities

3.1. Chief Information Security Officer (CISO)

Owns the Physical and Environmental Security Policy. Responsible for enterprise-level policy development, approval, and oversight. Coordinates with the CTO, CDO, and Facilities Management to ensure physical security controls align with the enterprise security architecture and risk posture.

3.2. Chief Technology Officer (CTO)

Co-designated (with the CISO) as the official responsible for managing the development,

documentation, and dissemination of the physical and environmental protection policy and procedures. Oversees infrastructure and operations teams responsible for facility-level implementation.

3.3. Deputy Chief, IT Operations

Responsible for the operational execution of physical access authorizations, facility access list management, and coordination with the Department of Capital Asset Management and Maintenance (DCAMM) for building access and credential management.

3.4. Agency Heads and Technical Support Managers (TSMs)

Responsible for ensuring agency-level compliance with this policy, including maintaining visitor logs, managing local access lists, securing agency-controlled areas, and reporting physical security incidents to ETSS.

3.5. Facilities Management / DCAMM

Responsible for building-level physical security infrastructure including access control systems, surveillance equipment, intrusion alarms, fire suppression systems, environmental controls, and emergency power systems. Coordinates with ETSS on security requirements for State-owned facilities.

3.6. All Personnel

Responsible for complying with physical access requirements, safeguarding authorization credentials, escorting visitors as required, reporting lost or stolen credentials, and reporting suspected physical security incidents promptly.

4. Procedures for Compliance

The following requirements establish the physical and environmental protection controls that agencies and ETSS must implement. Security controls are assigned based on the Information Assurance Level (IAL) of the information system, aligned to NIST SP 800-53 Rev. 5 Moderate baseline. Controls designated as applicable to all systems (IAL1 and IAL2) represent the minimum standard. Controls designated as IAL2 only apply to systems that store, process, transfer, or communicate classified data, including Personally Identifiable Information (PII), Federal Tax Information (FTI), or other sensitive data types.

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

Applies to: All systems (IAL1, IAL2)

Each agency shall develop, document, and disseminate a physical and environmental protection policy and supporting procedures to designated personnel identified in the applicable System Security Plan. The policy shall address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance requirements. The agency shall review and update the policy at least every three (3) years and following significant changes to facilities, the threat environment, or regulatory requirements. Supporting procedures shall be reviewed in alignment with the policy and updated following significant changes.

4.2 Physical Access Authorizations (PE-2)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Develop, approve, and maintain an Authorized Access List (AAL) of individuals permitted to access the facility where information systems reside. Physical access to areas containing classified data, including PII, shall be controlled through restricted areas, secured rooms, or locked enclosures.

b. Issue authorization credentials for access to non-public areas of the facility. ID badge access cards shall adhere to the DCAMM State Identification/Access Card Policy.

c. Review the AAL at least annually for state employees and at least quarterly for vendors and contractors.

d. Promptly remove individuals from the AAL when access is no longer required due to role change, separation, transfer, or termination.

4.3 Physical Access Control (PE-3)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Identify and designate public and non-public areas of the facility. Signs shall be posted to indicate restricted areas, but there shall be no signage indicating the location of information systems, computer rooms, or data centers. Information systems shall not be visible to a casual observer from outside the facility.

b. Implement appropriate safeguards such as cameras, security guards, and door or window locks to monitor and control access to non-public areas. For areas containing PII, at least two physical barriers shall be maintained under normal security conditions (for example, a secured perimeter combined with a locked container, or a locked perimeter combined with a secured interior).

c. Enforce physical access authorizations at controlled non-public areas by verifying each authorization prior to granting access and controlling facility entry and exit points using access control systems, devices, or security personnel.

d. Maintain physical access audit logs of individuals accessing controlled non-public areas.

e. Escort and monitor the activity of visitors who are not authorized for unescorted access. Visitors shall be accompanied at all times by authorized personnel within controlled non-public areas.

f. Secure keys, combinations, and other physical access devices from unauthorized access.

g. Perform an annual inventory of all physical access devices, including cipher locks, keys, keycards, and card readers.

h. Change cipher lock combination codes at least annually, after a suspected compromise, after a security violation in the controlled area, or when an individual with knowledge of the code no longer requires access.

i. Change or revoke keys and keycards when they are reported lost or stolen, after a security violation, or when the holder no longer requires access. Personnel shall return keys and keycards upon or prior to separation, transfer, or termination.

j. Maintain a list of personnel issued cipher lock combinations, keys, or keycards.

4.4 Access Control for Transmission (PE-4)

Applies to: Moderate and above (IAL2)

Each agency shall control physical access to information system transmission and distribution lines to authorized personnel only, in order to prevent accidental damage,

disruption, physical tampering, and eavesdropping on unencrypted transmissions. Wiring closets shall be locked, and unused physical ports within wiring closets and patch panels shall be disabled.

4.5 Access Control for Output Devices (PE-5)

Applies to: Moderate and above (IAL2)

Each agency shall protect and control access to information system output devices, including monitors, printers, copiers, and fax machines, to prevent unauthorized individuals from viewing or obtaining output. Output devices should be located within secured areas accessible only by authorized individuals. Where required by federal or state law or program compliance requirements, the agency should implement keypad or card reader access controls for output devices.

4.6 Monitoring Physical Access (PE-6)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Monitor physical access to the facility where information systems reside to detect and respond to physical security incidents.

b. Review physical access logs at least monthly for suspicious activity, including access outside of normal work hours, repeated access to areas not normally accessed, access of unusual duration, and out-of-sequence access.

c. Coordinate the results of physical access reviews with ETSS and the agency's incident response capability.

4.6.1 Intrusion Alarms and Surveillance Equipment (PE-6(1))

Applies to: Moderate and above (IAL2)

Each agency shall monitor and secure facilities housing information systems with physical intrusion alarms and surveillance equipment. The agency shall perform quarterly reviews of intrusion alarms and surveillance equipment to confirm their effectiveness during both normal business hours and when facilities are unoccupied.

4.7 Visitor Access Records (PE-8)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Maintain visitor access records for the facility where information systems reside in accordance with the State of Rhode Island General Records Retention Schedule GRS3.2, as required by federal or state law or regulatory compliance, or for a minimum of one (1) year, whichever is longer. Visitor records shall include, at a minimum, the visitor's name and organization, visitor signature (physical or electronic), form of identification, date of access, entry and departure times, purpose of visit, and the name and organization of the person visited. This requirement does not apply to publicly accessible areas.

b. Review visitor access records at least monthly.

c. Report anomalies in visitor access records to the Facilities Manager or agency Technical Support Manager (TSM).

4.8 Power Equipment and Cabling (PE-9)

Applies to: Moderate and above (IAL2)

Each agency shall protect power equipment and cabling for information systems from damage and destruction. This includes generators and power cabling located outside the facility, internal cabling and uninterruptible power supplies (UPS) located inside the facility, and HVAC systems. Only authorized maintenance personnel shall have access to this equipment.

4.9 Emergency Shutoff (PE-10)

Applies to: Moderate and above (IAL2)

Each agency shall install an emergency shutoff capability that:

a. Cuts power to the information system or individual system components in emergency situations.

b. Is located near an exit door in a safe and easily accessible location.

c. Is protected from unauthorized or inadvertent activation (for example, with a clear plastic cover).

4.10 Emergency Power (PE-11)

Applies to: Moderate and above (IAL2)

Each agency shall install an uninterruptible power supply (UPS) to facilitate an orderly shutdown of information systems or to support the transition to an alternate power source in the event of primary power loss. UPS maintenance shall be performed in accordance with the manufacturer's recommended schedule to maximize service life and ensure adequate backup power availability in alignment with business continuity requirements.

4.11 Emergency Lighting (PE-12)

Applies to: All systems (IAL1, IAL2)

Each agency shall install and maintain emergency lighting for emergency exits and evacuation routes that activates automatically in the event of a power outage or disruption.

4.12 Fire Protection (PE-13)

Applies to: All systems (IAL1, IAL2)

Each agency shall install, maintain, and periodically test fire suppression and detection systems for facilities housing information systems. Fire suppression systems should use environmentally safe suppression agents whenever possible. Water sprinkler systems are not an approved method of fire mitigation for areas containing information system equipment. Agencies should refer to the National Fire Protection Association (NFPA) for applicable standards and best practices.

4.12.1 Detection Systems with Automatic Activation and Notification (PE-13(1))

Applies to: Moderate and above (IAL2)

Each agency shall install and maintain fire detection and suppression systems that automatically activate and notify appropriate incident response and other designated personnel in the event of a fire.

4.13 Environmental Controls (PE-14)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Install temperature and humidity sensors in appropriate locations within the facility

where information systems reside.

b. Monitor and maintain temperature and humidity levels daily in accordance with manufacturer recommendations (generally approximately 70 degrees Fahrenheit and 50 percent relative humidity).

c. Alert designated personnel when sensors detect temperature or humidity levels outside of the acceptable range. Designated personnel shall report conditions and initiate remedial action, up to and including activation of contingency plan procedures, if necessary.

4.14 Water Damage Protection (PE-15)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Protect information systems from water damage by installing master shutoff valves and isolation zone valves (where appropriate) that are easily accessible.

b. Maintain master shutoff and isolation zone valves in proper operational condition.

c. Ensure key personnel know the locations of master shutoff and isolation zone valves.

4.15 Delivery and Removal (PE-16)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Authorize, monitor, and control information system components entering and exiting the facility. Enforcing authorizations may require restricting access to delivery areas and isolating those areas from information systems and media libraries.

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

4.16 Alternate Work Site (PE-17)

Applies to: Moderate and above (IAL2)

Each agency shall:

a. Identify and document alternate work sites allowed for use by employees.

b. Implement physical access controls at alternate work sites that provide safeguards and protections comparable to those at primary worksites.

c. Assess the effectiveness of controls at alternate work sites at least annually.

d. Provide a means for employees at alternate work sites to communicate with information security and privacy personnel in the event of a security incident.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include, but are not limited to:

a. Revocation or suspension of physical access credentials.

b. Mandatory retraining on physical security requirements.

c. Formal counseling or written reprimand.

d. Referral to agency management and human resources for disciplinary proceedings, up to and including termination of employment.

e. Termination of vendor or contractor agreements for third-party personnel.

f. Referral to law enforcement if criminal activity is suspected.

Non-compliance findings shall be documented and tracked through ETSS governance processes and may be recorded as findings in the agency Plan of Action and Milestones (POAM).

6. Approval / Review Signatures

Sanjay Gupta
Digitally signed by Sanjay Gupta
Date: 2026.06.22 16:36:45 -04'00'

Chief Technology Officer (CTO)
Division of Enterprise Technology Strategy and Services (ETSS)

Digitally signed by Nathan Loura
Date: 2026.06.23 12:16:43 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services (ETSS)

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.06.23 12:42:21 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services (ETSS)