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 Departments\(^1\) (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, 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, maintain, and semi-annually review an AAL,
2. Issue authorization credentials for access to non-public areas of the facility in accordance with DCAMM State Identification/Access Card Policy,
3. Promptly remove individuals from the AAL when access is no longer required.

### 4.3. [IAL1, IAL2] Physical Access Control (PE-3)

The agency will:
- Identify public and non-public areas of the facility. Non-public areas will be designated, controlled, and appropriately secured. 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.
- Enforce physical access authorizations to controlled non-public areas of the facility by verifying each access authorization prior to granting access to the facility and using an access control system/device or security guard to control entry/exit points. Only authorized personnel are allowed access to controlled non-public areas.
- Maintain physical access audit logs of individuals accessing controlled non-public areas of the facility.
- Implement appropriate safeguards (e.g. cameras, security guards, auto-locking doors) to monitor and control access to publicly accessible areas within the facility.
• Escort and monitor the activity of visitors, including vendors, contractors, maintenance, and facilities personnel, not authorized to access 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.
• Secure keys, combinations to locks, and other physical access devices from unauthorized access.
• Inventory all physical access devices (e.g. keys, key cards, card readers) annually.
• Cipher lock combination codes will be changed no less than annually and whenever there is an actual or suspected incidence of a compromised code. Keys and key cards will be changed whenever they’re reported as being lost or stolen. Keys, key cards, and cipher lock combination codes will be promptly changed whenever there is a theft or security violation within the area being protected or an employee with knowledge of the combination code (or has been assigned a key) is transferred, terminated, or no longer requires access. The agency will maintain a list of personnel issued keys, key cards, and cipher lock combination codes. Personnel will promptly return assigned keys and key cards to the agency upon or prior to separation, transfer, or termination.

4.4. [IAL1, IAL2] Access Control for Transmission Medium (PE-4). The agency will control physical access for information system transmission and distribution lines within agency facilities to help prevent accidental damage, disruption, physical tampering, and eavesdropping of unencrypted transmissions. For example, restricting access to secure areas (e.g. electronic ID badge permissions, lock entrance to restricted areas, video surveillance monitoring), locking wiring closets and protecting cabling by conduit or cabling trays.

4.5. [IAL2] Access Control for Output Devices (PE-5). The agency will protect and control physical access to information system output devices (e.g. monitors, printers, copiers, scanners, fax machines, audio devices) to prevent unauthorized individuals from obtaining the output. For example, placing output devices within locked rooms or secured areas that can only be accessed by authorized individuals and monitored by agency personnel.

4.6. [IAL1, IAL2] Monitoring Physical Access (PE-6). The agency will (i) monitor physical access to the facility where the information system resides to detect and respond to physical security incidents, (ii) review physical access logs at least quarterly 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, and (iii) coordinate results of reviews with the agency incident response capability.

4.6.1. [IAL2] Intrusion Alarms and Surveillance Equipment (PE-6.1). The agency will monitor and secure physical intrusion alarms and surveillance equipment. The agency will perform quarterly reviews of 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 (i) maintain visitor access records to the facility for a minimum of one (1) year or as required by federal or state mandate or regulatory compliance requirement, whichever is longer, and (ii) review visitor access records on an annual basis. See RI General Records Retention Schedule GRS3.2 (https://www.sos.ri.gov/assets/downloads/documents/GSR3-safety-and-security-records.pdf) for more information regarding visitor access record retention schedules.

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 and internal cabling and uninterruptable power supplies (UPS) located inside the facility.

4.9. [IAL2] Emergency Shutoff (PE-10). The agency will install an emergency shutoff switch that (i) cuts power to the information system or individual system components in emergency situations, (ii) is located near an exit door in a safe location easily accessible by personnel, and (iii) is protected from unauthorized or inadvertent activation (e.g. see-through 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 the primary power source is lost.

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.


4.12.1. [IAL2] Automatic Fire Suppression (PE-13.3). The agency will install, maintain, and periodically test an automatic fire suppression system and detection devices for the information system when the facility is not staffed on a continuous basis.

4.13. [IAL1, IAL2] Temperature and Humidity Controls (PE-14). The agency will install temperature and humidity sensors in appropriate locations within the data center where the information system resides. Data center temperature and humidity levels will be monitored and maintained at appropriate levels (approximately 70°F and 50% humidity).
Designated personnel will be automatically alerted when sensors detect temperature or humidity levels that are out of range.

4.14. [IAL1, IAL2] Water Damage Protection (PE-15). The agency will (i) protect the information system from water damage by installing a master shutoff and isolation zone valves (where appropriate) that are easily accessible, (ii) maintain master shutoff and isolation zone valves in proper operational condition, and (iii) ensure key personnel know where master shutoff and isolation zone valves are located.

4.15. [IAL1, IAL2] Delivery and Removal (PE-16). The agency will (i) protect the information system from water damage by installing a master shutoff and isolation zone valves (where appropriate) that are easily accessible, (ii) maintain master shutoff and isolation zone valves in proper operational condition, and (iii) ensure key personnel know where master shutoff and isolation zone valves are located.

4.16. [IAL2] Alternate Work Site (PE-17). The agency will (i) implement physical access security controls at alternate work sites that provide similar safeguards and protections as primary worksites, (ii) annually assesses the effectiveness of security controls at alternate work sites, and (iii) provide a means for employees to communicate with information security personnel in the event of a security incident.

4.17. [IAL2] Location of Information System Components (PE-18). The agency will position information system components within the facility to minimize the opportunity for unauthorized access and the potential damage from natural and man-made physical and environmental hazards, including flooding, fire, tornados, earthquakes, hurricanes, vandalism, unauthorized access, electronic interception of transmissions, electrical interference, and various forms of electromagnetic radiation.

4.18. [IAL1, IAL2] Asset Monitoring and Tracking (PE-20). The agency will employ asset location technology to track and monitor the location and movement of state-owned vehicles and critical information system components to ensure they remain within authorized locations.

5. Approval / Review Signature

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2020.09.14 12:00:15 -04'00'

Chief Information Security Officer