



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-10-16-2014

DIVISION OF INFORMATION TECHNOLOGY

Physical and Environmental Security Policy

Date of Last Revision 07/31/2014

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Background

- a. Physical and environmental security controls protect information system facilities from physical and environmental threats. Physical access to facilities and supporting infrastructure, such as communications, power, and cabling, must be secured to prevent their compromise.

2. Purpose

- a. To establish a Physical and Environmental Security Policy that effectively protects information systems and information system components from physical and environmental hazards.

3. Scope

- a. This policy covers all State Executive Branch Departments¹ (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

4. Authority

- a. Executive Order 04-06 established the Division of Information Technology (DoIT) within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive Branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5. Definitions

- a. **Emergency Controls** - Systems or system components that provide for continued control, or that can be activated to provide enhanced control, in the event of an emergency.

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

- b. Environmental Controls** - Systems or system components that ensure a stable operating environment with respect to the environment, such as temperature, humidity, water levels, etc.
- c. Physical Access** - The process by which a person may corporeally be present in a given area or location.
- d. Waiver** - A dispensation from policy due to extenuating circumstances.

6. Policy

a. Physical Access Authorizations.

- (i.)** An access control list of personnel authorized to physically access the information system facility will be developed, approved, maintained current, updated to reflect individuals no longer requiring access, and periodically reviewed.
- (ii.)** Authorization credentials will be issued for physical access to information system facilities. Different credentials may be required for different information system facilities and persons/entities may be required to sign certain documents before entrance.

b. Physical Access Controls.

- (i.)** Physical access authorizations will be controlled and verified at information system facility entrances prior to granting access.
- (ii.)** Physical access logs for all personnel, including visitors, accessing information system facilities will be maintained and periodically reviewed.
- (iii.)** Physical access to information system facilities will be monitored to detect and respond to physical security incidents. Visitors will be escorted and their activities will be monitored while within controlled areas of information system facilities.
- (iv.)** Publicly accessible areas within information system facilities will be designated, controlled, and secured.
- (v.)** Devices that control physical access to information system facilities will be secured and periodically inventoried.
- (vi.)** Cipher lock combination codes will be changed annually, whenever there is an actual or suspected incidence of a compromised code, or personnel knowing the combination are transferred or terminated. Keys and/or card keys will be changed whenever reported as being lost or personnel having keys and/or card keys are transferred or terminated.
- (vii.)** Physical access to distribution lines, transmission lines, output devices, and other power equipment and cabling critical to the functionality of information systems will be secured, restricted to authorized users/individuals, and protected from damage.
- (viii.)** Information system components entering and leaving information system facilities will be authorized, monitored, documented, and controlled.

- (ix.) Physical access to alternate work sites will be secured, periodically assessed, and provide a means to communicate with information security personnel in the event of an incident.
- (x.) Information system components will be positioned within facilities to minimize the opportunity for unauthorized access and the potential damage from physical and environmental hazards.

c. Emergency Controls.

- (i.) An emergency shutoff switch that cuts power to information systems and/or individual system components in emergency situations will be installed, be easily accessible to personnel, and be protected from unauthorized or inadvertent activation.
- (ii.) An uninterruptible power supply will be installed in order to facilitate an orderly information system shutdown or to transition to an alternate power source in the event the primary source of power is lost.
- (iii.) Emergency lighting that is automatically activated in the event of a power outage or disruption will be installed.

d. Environmental Controls.

- (i.) Fire suppression and detection systems and devices that are maintained and periodically tested will be installed at information system facilities.
- (ii.) Temperature and humidity levels at information system facilities will be monitored and maintained at appropriate levels.
- (iii.) Information systems will be protected against water damage.

e. Policy Issuance. This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be amended or revoked.

f. Policy Reviews. This policy will be reviewed annually and updated as required.

g. Noncompliance. Any person or entity that violates this policy shall be subject to disciplinary action up to and including termination.

h. Waivers. The Agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, or upon the ending for the reason for the waiver, whichever occurs first, whereupon they must be renewed.

7. Roles and Responsibilities

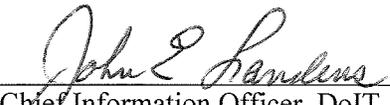
a. Chief Information Security

- (i.) Periodically review and update this policy, as required.
- (ii.) Periodically assess physical and environmental security at Agency information system facilities to ensure compliance with this policy.

b. Agency

- (i.) Comply with provisions documented in this policy.
- (ii.) Maintain a list of personnel authorized to access information system facilities.
- (iii.) Issue credentials for physical access to information systems.
- (iv.) Log all access to information system facilities.
- (v.) Ensure physical and environmental controls are in place to secure information system facilities.

8. Signatures



Chief Information Officer, DoIT

11/25/2014

Date



Chief Information Security Officer, DoIT

11/24/2014

Date



Director, Department of Administration

12-3-14

Date