

# 9100-P150 – Physical Security of IT Resources

## I. PURPOSE

Physical security is an essential control to ensure the confidentiality, integrity, and availability of state information. This policy establishes requirements for physical security controls for State and agency data centers and information technology (IT) resources within or external to those data centers.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”).

## III. POLICY

### A. Agency Data Centers

Agency heads, in coordination with the facility managers, shall designate data centers within their areas of responsibility and ensure that physical security is addressed.

1. Security perimeters (e.g., walls, gates, locked doors, etc.) shall be used to isolate and protect data centers.
2. Public areas and other points (e.g., exterior doors, loading docks, etc.) that could be used by unauthorized persons to enter data centers or facilities that process restricted information shall be controlled and monitored.
3. Access controls shall be employed to ensure that only authorized personnel are allowed into data centers. These controls shall be routinely monitored for effectiveness.
4. Methods shall be implemented to identify/distinguish data center employees from authorized data center visitors.
5. Environmental controls shall be applied to ensure that systems operate within vendor-specified conditions. Environmental controls shall be monitored and maintained in accordance with vendor recommended service intervals and specifications.
6. Uninterruptible power supplies (UPS) and/or generators shall be capable of providing continuous power for a specified period of time to meet availability requirements or to allow for an orderly shutdown to prevent damage or corruption of the data.
7. Fire suppression systems, emergency power down switches, and emergency lighting shall be installed and operational in all data centers.

## 9100-P150 – Physical Security of IT Resources

8. Procedures for responding to environmental emergencies shall be posted within data centers and personnel in the facility shall be trained on their responsibilities.

### B. State IT resources

All state IT resources shall have appropriate physical protection from security threats and environmental hazards to prevent the loss, damage, or compromise of assets, and interruption to business activities.

1. Physical protections normally afforded to IT resources within a data center shall be considered for IT resources outside of a data center when the data steward or data owner considers such protection to be appropriate.
2. Physical isolation of servers that process or store restricted information shall be a business consideration addressed by the IT resource owner.

### C. Physical Security of the Network

The physical IT resource infrastructure shall be protected. Protective controls commensurate to the risk of losing confidentiality, integrity, or availability shall be applied to the physical components of the network.

1. New power and telecommunications cabling (to include wireless devices) shall be protected where possible, from interception or damage with controls such as conduit, locked rooms, or locked boxes at inspection and termination points.
2. All equipment and cables shall be clearly marked at connection points and network diagrams shall be kept updated to correspond to these markings.

### D. Repairs

Only authorized personnel shall carry out repairs or service agency IT resources. Records of preventive and corrective maintenance shall be maintained by personnel responsible for the equipment as long as the equipment is in use.

### E. Off-site locations

State information and/or IT resources that are stored or used off-site shall be accounted for and given the same level of protection as those found on-site. If the off-site location cannot provide the required level of protection, the agency head or designee and the end-user shall be jointly responsible for risk mitigation (see Policy 9400-P175 – Mobile Computing and Telework).

## **9100-P150 – Physical Security of IT Resources**

### F. Compliance

The presence and effectiveness of physical controls shall be reviewed on a regular basis. Agency heads shall evaluate the adequacy of controls, identify potential gaps, develop mitigating controls, and work with those responsible for securing the areas to determine long-term corrective action.

**CIO Approved Date: 1/5/2011**