State of Vermont

Physical Security for Computer Protection Policy

Date Approved: 04-02-10
Approved by: Tom Pelham
Policy Number: 0501.012005

Contents

1.0 Introduction

1.1 Authority

The State of Vermont is authorized to undertake the development of enterprise architecture policies and standards. The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), “to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government.”

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

State office locations that include computers and other types of information technology resources must be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at entrances, security guards, and fire protection.

Information Security issues to be considered are:

- Unlawful access may be gained with the intent of theft, damage, or other disruption of operations.
- Unauthorized and illegal access may take place covertly (internal or external source) to steal, damage, or otherwise disrupt operations.
- Destruction or damage of physical space may occur due to environmental threats such as fire, flood, wind, etc.
- Loss of power may result in the loss of data, damage to equipment and disruption of operations.

1.3 Scope

This policy addresses threats to critical IT resources that result from unauthorized access to facilities owned or leased by the State of Vermont, including offices, data centers and similar facilities that are used to house such resources.

2.0 Policy

All information resource facilities must be physically protected in proportion to the criticality or importance of their function. Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

2.1 Use of Secure Areas to Protect Data and Information

- Use physical methods to control assess to information processing areas. These methods include, but are not limited to, locked doors, secured cage areas, vaults, ID cards, and biometrics.
- Restrict building assess to authorized personnel.
- Identify areas within a building that should receive special protection and be designated as a secure area. An example would be a server room.
- Use entry controls.
- Security methods should be commensurate with security risk.
- Ensure that physical barriers are used to prevent contamination from external environmental sources. For example: Water tight walls in flood zones. Proper ventilation in areas exposed to chemical vapors.
- Compliance with fire codes.
- Installation, use and maintenance of air handling, cooling, UPS and generator backup to protect the IT investment within data rooms.

2.2 Physical Access management to protect data and information

- Access to facilities that house critical state IT infrastructure, systems and programs must follow the principle of least privilege access. Personnel, including full and part-time staff, contractors and vendors' staff should be granted access only to facilities and systems that are necessary for the fulfillment of their job responsibilities.
- The process for granting physical access to information resources facilities must include the approval of the CIO, or his or her designee. Access reviews must be conducted at least quarterly, or more frequently depending on the nature of the systems that are being protected. Removal of individuals who no longer require access must then be completed in a timely manner.

- Access cards and keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.
- Security clearance for visitors. This could include, but is not limited to, a sign in book, employee escort within a secure area, ID check and ID badges for visitors.

3.0 Policy Notification

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.