Table of Contents

1. Purpose

This policy establishes the physical protection requirements for facilities used for processing cardholder data. It covers all network components, computers (servers, laptops, desktops) and external peripherals.

2. Scope

The scope of this policy includes areas housing agency network components, computers (servers, laptops, desktops). The Agency is responsible for maintaining the security of information technology (IT) equipment.

3. Policy

3.1. Physical Security

Department 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.

3.1.1. Information Security issues:

- 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.

3.1.2. Physical access management:

- The process for granting physical access to information resources facilities must include the approval of the Chief Information Office, their designee or other responsible and assigned party. Access reviews must be conducted at least quarterly. Removal of individuals who no longer require access must be completed in a timely manner.
- Access cards must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards must be reported immediately to the employee’s supervisor and security.
- Security clearance for visitors. This includes a sign in book, employee escort within a secure area, and ID badges for visitors.

3.1.3. Visitor Access

Visitors shall:

1. Visitors are to enter via the main public doors.
2. Check in with the front desk/lobby before entering a physically secure location by:

   a. Provide a form of identification used to authenticate visitor.
   b. Be issued a visitor badge, the visitor badge shall be worn on visitor's outer clothing and collected at the end of the visit.
   c. Sign the visitor's log listing their name, organization, who they are seeing, date/time of arrival, visitor badge number, date/time of departure.

3. Be accompanied by an escort at all times. An escort is defined as authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.
4. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, agency law enforcement personnel shall be notified or call 911.
5. If any of the exceptions identified in #4 above occur, the employee sponsoring the offending visitor will not be allowed to sponsor another visitor.
6. Photographs of IT areas are not allowed without permission of the CIO.

3.1.4. Environmental and life safety controls

The following controls should ensure that operation of the equipment in the computer room and telecommunications closets can be maintained and that personnel safety controls are in place.

3.1.4.1. Site Perimeter

- All doors on the outside of the building except the public entrance should have badge readers for authorized employees. Doors from the public area (lobby) to other parts of the building should have badge reader enabled doors. The badge reader database should record the date/time, person, and location of each door being accessed. Access via key should only be used in emergency situations or failures of the badge reader system. Keys should be issued only to a limited number of people who are responsible for the building.

3.1.4.2. Computer Rooms and Telecommunications Closets

3.1.4.2.1. Windows

- No windows to the outside.

3.1.4.2.2. Doors

- Badge readers for authorized employees. The badge reader database should record the date/time, person, and location of each door being accessed.
- Access via key should only be used in emergency situations or failures of the badge reader system. Keys should be issued only to a limited number of people who are responsible for the computer rooms and telecommunications closets. Cleaning personnel should not be issued keys.

- If keys are used a log should be maintained. Additionally, lock should be changed periodically to insure integrity of the keyed system.
- Fireproof
- No more than two doors to a computer room and one to a telecommunications closet.

3.1.4.2.3. Infrastructure

- Monitored via CCTV cameras
- Alarmed for unauthorized intrusions
- Unless exempted, at least an 18" access floor to provide for air flow and cable management
- Air filtration system
- High ceilings to allow for heat dispersal.

3.1.4.2.4. Electrical Power

- Receive steady electrical power to sustain the operation of the servers and electrical equipment within the room.
- Two separate electrical power supplies
- UPS (uninterruptible power supply) system
- Diesel backup should be installed to address longer-term blackouts
- Interruptions should provoke an alarm and inform ISD and facilities management immediately.

3.1.4.2.5. Fire detection and suppression

- Halon or other total flooding agent
- Fire extinguisher
- Emergency power off switches
- Must not contain a wet pipe sprinkler system
- Air tight room

3.1.4.2.6. Air Conditioning

- Temperature between 55 and 75 degrees Fahrenheit
- Humidity of between 20 and 80 percent
- Environmental sensors should log the temperature and humidity of the room and report it to ISD for monitoring and trend analysis

3.1.4.2.7. Cleaning

- Cleaning personnel should be instructed what they are allowed to do and where they should pay attention
- Must be escorted by ISD personnel

3.1.5. Physical Control

3.1.5.1. Computer Inventory Control

- Servers and equipment within the computer room should be checked daily (business days) on functionality and existence.

- Machines have to be checked that they work properly and that there is no damage to the devices.
- All devices are still in place and no theft has occurred.

3.1.5.2. Computer Labelling

- Each computer and all equipment inside the room should be labelled.
- Label information should include IP address and server name.
- State of New Mexico property tags
- Asset tags as needed

3.1.5.3. Media Storage Requirements

- Media should be stored in fire proof safe to protect it from unintentional events like fire or water and from intentional events like theft or vandalism.
- Backup files via tape should be performed and kept off-site.

3.1.5.4. Workstation and External Drive Devices Physical Security

- Systems that contain sensitive information must be either:
  - Physically attached via a secure locking device to some relatively immobile object
  - Housed in an area that uses access control systems (e.g., card-key, crypto-lock)
  - Be encryption enabled when not in use

3.1.5.5. Credit Card Processing

- POS terminals are used to process credit cards and must be:
  - If stationary, physically attached via a secure locking device to some relatively immobile object
  - If mobile devices, should be kept in secure storage when not in use (e.g., locked in a cabinet, tethered to a counter or under 24-hour surveillance).
  - Housed in an area that uses access control systems (e.g., card-key, crypto-lock)
  - Shut down during non-business hours
  - Usage observed via CCTV cameras
  - Inspected monthly to validate the POS terminal has not been altered
- Computers used to perform credit card transactions must be:
  - Usage observed via CCTV cameras
  - Be screen locked when unattended
  - Logged off during non-business hours