Physical Security Policy

January 29, 2025

GTEL Advisors, LLC

6120 Berkshire Lane North
Plymouth, Minnesota 55446
Phone: 612-386-4141
1/29/2025

Table of Contents

1. Introduction....2
2. Purpose of the Policy....2
3. Scope....2
4. Governance and Compliance....3
4.1 NIST Cybersecurity Framework....3
4.2 Criminal Justice Information Security Compliance....3
5. Physical Security Requirements....3
5.1 Facility Access Control....3
5.2 Protection of Computer Equipment....4
5.3 Environmental Controls....4
5.4 Surveillance and Monitoring....4
6. Personnel Security....5
6.1 Employee and Contractor Screening....5
6.2 Physical Security Training and Awareness....5
7. Emergency Procedures....5
7.1 Fire and Hazard Response....5
7.2 Disaster Recovery and Backup Plans....5
8. Audit and Compliance....5
8.1 Regular Security Audits....5
8.2 Compliance with Criminal Justice Information Security Policy....6
9. Policy Violations and Enforcement....6
9.1 Violations and Disciplinary Actions....6
9.2 Reporting and Investigation....6

1. Introduction

[Agency Name] recognizes the importance of protecting its computer facilities to maintain the confidentiality, integrity, and availability of information, particularly for sensitive data, such as Criminal Justice Information (CJI). This Physical Security Policy establishes a framework for ensuring that all computer facilities housing sensitive systems and data are secured in accordance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Criminal Justice Information Services (CJIS) Security Policy. This policy applies to all employees, contractors, and other individuals who access [Agency Name]'s computer facilities.

2. Purpose of the Policy

The purpose of this policy is to establish guidelines and procedures for securing physical access to computer facilities, protect hardware, and ensure the integrity of data and systems. Specific objectives include:

- Safeguarding physical access to critical systems that store, process, or transmit sensitive data, including Criminal Justice Information (CJI).
- Preventing unauthorized access to physical infrastructure that could compromise the security of data or systems.
- Ensuring compliance with the NIST Cybersecurity Framework and CJIS Security Policy regarding physical security controls.
- Protecting the organization from physical threats such as theft, vandalism, environmental hazards, and natural disasters.

3. Scope

This policy applies to all employees, contractors, consultants, and third-party vendors who access or manage [Agency Name]'s computer facilities. It applies to all physical locations where agency-owned or managed computer systems, data storage devices, and networking equipment are housed, including:

- Data centers
- Server rooms
- IT storage areas
- Any location where sensitive data or systems are stored, processed or transmitted

4. Governance and Compliance

4.1 NIST Cybersecurity Framework

[Agency Name] aligns its physical security practices with the NIST Cybersecurity Framework (CSF) to ensure the protection of systems, assets, and data. Key functions from the NIST CSF that are incorporated into this policy include:

- Identify: Understand the assets, systems, and data that need protection and assess the associated physical security risks.
- Protect: Implement physical access controls, secure facilities, and apply environmental protections to safeguard critical resources.
- Detect: Monitor and detect unauthorized physical access or security events in the computer facility.
- Respond: Develop and implement procedures for responding to security incidents related to physical security breaches.
- Recover: Establish plans for recovery in the event of a physical security breach or environmental disaster.

4.2 Criminal Justice Information Security Compliance

Given that [Agency Name] may handle or have access to Criminal Justice Information (CJI), it is critical that physical security practices comply with the Criminal Justice Information Services (CJIS) Security Policy. The CJIS Security Policy outlines specific physical security requirements, including:

- Limiting physical access to facilities and systems that store or process CJI.
- Ensuring that all personnel with access to CJI undergo appropriate background checks and training.
- Implementing controls to protect CJI during both physical and electronic transmission.

Compliance with the CJIS Security Policy ensures that [Agency Name] remains aligned with national standards for protecting criminal justice data.

5. Physical Security Requirements

5.1 Facility Access Control

Access to computer facilities must be strictly controlled to ensure that only authorized personnel can enter restricted areas. Controls include:

- Access Authorization: Only authorized personnel, such as system administrators and IT staff, may be granted access to computer facilities. Access should be based on the principle of least privilege.
- Access Control Systems: Use of card readers, biometric systems, or other access control methods to limit entry to designated personnel.

- Visitor Access: Visitors or contractors must be escorted at all times within restricted areas. Visitors should sign in and out of the facility and be subject to background checks as necessary.

5.2 Protection of Computer Equipment

Physical protection of computer hardware and data storage devices is essential to prevent theft, tampering, or unauthorized access. This includes:

- Locking Enclosures: All servers, network equipment, and storage devices should be housed in locked cabinets or enclosures to prevent unauthorized tampering.
- Access to Equipment: Only authorized individuals should have access to equipment in the facility, and access should be logged for auditing purposes.
- Physical Security Devices: Use of cable locks, rack-mounted security enclosures, and other mechanisms to secure devices against physical theft or damage.

5.3 Environmental Controls

To prevent damage or disruption caused by environmental factors, the following controls should be implemented:

- Fire Suppression: Installation of fire detection and suppression systems (e.g., smoke detectors, automatic sprinkler systems, and fire extinguishers) to protect critical IT equipment.
- Temperature and Humidity Control: Use of temperature and humidity monitoring systems to ensure that environmental conditions remain within safe operating ranges for sensitive equipment.
- Power Management: Use of uninterruptible power supplies (UPS) and backup generators to ensure continuous power in case of electrical outages.

5.4 Surveillance and Monitoring

Monitoring of computer facilities is crucial to detect unauthorized access or suspicious activity. This includes:

- Surveillance Cameras: Installation of security cameras around the perimeter and inside the facility, especially in areas housing sensitive data or equipment.
- Alarm Systems: Integration of motion detectors and door/window sensors connected to a central alarm system to alert security personnel to any unauthorized access attempts.
- Continuous Monitoring: 24/7 monitoring of security systems to ensure rapid detection and response to potential physical security incidents.

6. Personnel Security

6.1 Employee and Contractor Screening

Employees and contractors who require access to computer facilities should undergo appropriate background checks to ensure they are trustworthy and do not pose a security risk. These checks should include:

- Criminal background checks.
- Security clearance (if applicable).
- Verification of employment history and references.

6.2 Physical Security Training and Awareness

All personnel who are authorized to access computer facilities must receive training on physical security procedures, including:

- Proper use of access control systems.
- Reporting security incidents or suspicious activity.
- Emergency procedures in the event of fire, power failure, or natural disaster.
- Handling of sensitive or criminal justice data to prevent unauthorized access.

7. Emergency Procedures

7.1 Fire and Hazard Response

[Agency Name] will establish emergency response protocols for fire, flood, and other environmental hazards. This includes:

- Clearly marked emergency exits.
- Regular fire drills to ensure personnel are familiar with evacuation routes.
- Fire suppression systems in place to protect critical infrastructure.

7.2 Disaster Recovery and Backup Plans

In the event of a disaster or physical breach, the agency must:

- Maintain offsite backups of critical data and systems.
- Implement disaster recovery plans to ensure quick restoration of services.
- Regularly test backup and recovery processes to ensure effectiveness.

8. Audit and Compliance

8.1 Regular Security Audits

Regular security audits of the physical security controls must be conducted to ensure compliance with this policy and identify any vulnerabilities. Audits should be performed annually or after significant changes to the facility or systems.

8.2 Compliance with Criminal Justice Information Security Policy

[Agency Name] will conduct periodic assessments to ensure that its physical security controls comply with the CJIS Security Policy. Non-compliance with this policy could result in a loss of access to Criminal Justice Information.

9. Policy Violations and Enforcement

9.1 Violations and Disciplinary Actions

Any violations of this policy, including unauthorized access or tampering with security systems, will result in disciplinary action, including potential termination of employment or contracts.

9.2 Reporting and Investigation

Any suspected violations should be immediately reported to security personnel or management. All reports will be thoroughly investigated, and corrective actions will be taken to prevent future violations.