

Example Physical Security Policy

This is an example physical security policy. Use this as a guide to write or revise the physical security policy for your organization.

~~~~~

## Physical Security Policy

### 1.0 Purpose

The purpose of this policy is to protect the organization's physical and information assets by ensuring robust physical security measures are in place, safeguarding against unauthorized access, and complying with relevant laws and regulations.

### 2.0 Scope

This policy applies to all employees, contractors, and third-party vendors. It encompasses all organizational facilities, information systems, and data.

### 3.0 Policy

#### 3.1 Physical Access Controls

- Access control measures, including physical barriers such as locks, fences, and security doors, will be implemented based on the classification of information stored at each location.
- Access to all offices, computer rooms, and work areas containing sensitive information shall be physically restricted to individuals with a demonstrated need to know.
- Unauthorized entry into restricted areas within organization buildings is strictly prohibited.
- Procedures for granting, modifying, and revoking physical access shall be developed and implemented.

#### 3.2 Visitors

- All visitors must sign a log before gaining access beyond the reception area.
- A visitor log will be maintained, recording each visitor's name, date of visit, and purpose, as well as entry and exit times.
- Visitors, including customers, vendors, former employees, contractors, and others, must always be escorted by authorized employees while on organization premises.

- Unescorted visitors found on organization premises must be questioned and accompanied to the reception area or the person they came to see.
- Visitors violating this policy are subject to loss of vendor privileges and termination of services from the organization.

### **3.3 Workstation Security**

- Only authorized users can use organization workstations to complete assigned tasks.
- All users must monitor workstations and report unauthorized access.

### **3.4 Surveillance**

- Surveillance cameras must be installed in critical areas to monitor and record activities. Recorded footage must be stored securely and reviewed as needed, particularly in response to specific incidents or suspicious activities.

### **3.5 Emergency Procedures**

- Clear emergency procedures must be established and communicated to all users, including evacuation routes and emergency contacts.

### **3.6 Review**

- A comprehensive review of physical security controls will be conducted annually.

### **3.7 Reporting of Security Incidents**

- Users must immediately report security incidents, including unauthorized access, theft, or suspicious activities, to their manager and the security officer.

## **4.0 Responsibilities**

### **Employees**

- Follow all physical security protocols and immediately report any security incidents or suspicious activities

### **IT Department**

- Implement and maintain physical security controls for all IT equipment and data centers

### **Managers**

- Ensure their teams understand and adhere to the physical security policy and conduct regular training sessions

### **Security Officer**

- Oversee the physical security strategy, conduct regular audits, and enforce policy compliance

## 5.0 Compliance

Compliance with this policy is mandatory for all employees, contractors, and stakeholders. Noncompliance may result in disciplinary actions, including termination of employment, and could lead to legal consequences if it involves violations of laws and regulations.

## 6.0 Enforcement

This policy will be enforced with regular audits and continuous monitoring conducted by the security officer. Any violations of the policy will be subject to thorough investigation, and appropriate disciplinary measures will be taken based on the severity of the noncompliance. Actions may include warnings, retraining, suspension, or termination, depending on the nature of the violation.

## 7.0 Definitions

- **Access control:** mechanisms that restrict entry to authorized individuals only
- **Visitor management:** procedures for handling and monitoring visitors within the organization
- **Surveillance:** monitoring activities through cameras or other recording devices

## 8.0 Review and Updates

This policy will be reviewed annually or as needed to ensure its relevance and effectiveness. The security officer is responsible for coordinating the review and update process. A revision history will be maintained to document changes and updates.

### Revision History

| Date       | Description of Change                    | Changed By     |
|------------|------------------------------------------|----------------|
| YYYY-MM-DD | [Initial draft or specific changes made] | [Name or role] |