Physical Security Policy Template

Document Control Information

- **Document Title:** Physical Security Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Physical Security Policy establishes [ORGANIZATION NAME]'s requirements for protecting physical areas, equipment, and information assets from unauthorized access, damage, theft, compromise, or interference in accordance with ISO 27001:2022 requirements. It provides a framework for implementing and maintaining physical security controls to protect the organization's facilities and assets.

1.2 Scope

This policy applies to: - All physical locations owned, leased, or managed by [ORGANIZATION NAME] - All equipment, systems, and information assets within these locations - All employees, contractors, consultants, visitors, and other individuals accessing these locations - All physical security systems and controls implemented by the organization - All hours of operation, including normal business hours and after-hours periods

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing appropriate physical security controls based on risk assessment - Protecting facilities, equipment, and information from physical threats - Preventing unauthorized physical access to sensitive areas - Ensuring business continuity through physical security measures - Complying with relevant legal, regulatory, and contractual requirements - Regularly reviewing and improving physical security controls

2. Physical Security Perimeters

2.1 Security Perimeter Definition

- Physical security perimeters shall be defined and documented
- Perimeters shall be based on security requirements and risk assessment
- Multiple perimeters may be established for different security levels
- Perimeter boundaries shall be clearly identifiable
- Perimeters shall be regularly reviewed and updated as needed

2.2 Perimeter Security Controls

- Perimeter walls, doors, and windows shall be of solid construction
- External doors and accessible windows shall be protected against unauthorized access
- Fire doors shall be alarmed, monitored, and tested
- Intruder detection systems shall be installed where appropriate
- Security personnel shall monitor perimeters where necessary
- Physical barriers shall extend from floor to ceiling where required

2.3 Reception and Public Access Areas

- Reception areas shall be staffed during business hours
- Visitor access shall be controlled at reception points
- Public access areas shall be separated from restricted areas
- Deliveries shall be received in designated areas
- Public access areas shall be monitored by CCTV where appropriate
- Emergency exits shall be secured while allowing safe evacuation

3. Physical Entry Controls

3.1 Access Control Systems

- Access control systems shall be implemented for restricted areas
- Access control may include:
    - Electronic access cards or tokens
    - Biometric authentication
    - PIN codes
    - Keys and locks
    - Security personnel
- Access control systems shall be regularly maintained and tested
- Access logs shall be maintained and reviewed

3.2 Access Authorization

- Access to secure areas shall be authorized and documented
- Access rights shall be based on job requirements and need
- Access authorization shall be approved by area owners
- Access rights shall be regularly reviewed and updated
- Temporary access shall be time-limited and monitored
- Access rights shall be promptly revoked when no longer required

3.3 Visitor Management

- Visitors shall be required to sign in and out
- Visitor identification shall be verified
- Visitors shall be issued temporary identification
- Visitors shall be escorted in restricted areas
- Visitor access shall be limited to required areas only
- Visitor logs shall be maintained and reviewed
- Visitor procedures shall be clearly communicated

3.4 Access Monitoring and Logging

- Access to secure areas shall be logged and monitored
- Logs shall include:
    - Identity of individual
    - Date and time of entry and exit
    - Purpose of visit (for visitors)
    - Escort information (if applicable)
- Logs shall be protected from tampering
- Logs shall be retained according to retention policies
- Unusual access patterns shall be investigated

4. Securing Offices, Rooms, and Facilities

4.1 Office Security

- Offices shall be locked when unoccupied
- Sensitive information shall be secured when not in use
- Clear desk and clear screen policies shall be implemented
- Office layouts shall consider security requirements
- Unattended areas shall be physically secured
- Office security shall be regularly assessed

4.2 Secure Areas

- Secure areas shall be established for sensitive operations
- Secure areas may include:
  - Data centers
  - Server rooms
  - Network equipment rooms
  - Security operations centers
  - Sensitive document storage
- Secure areas shall have additional access controls
- Secure areas shall be physically separated from public areas
- Working in secure areas shall be supervised and monitored

4.3 Equipment Rooms

- Equipment rooms shall be secured against unauthorized access
- Equipment rooms shall be protected from environmental threats
- Access to equipment rooms shall be restricted and logged
- Equipment rooms shall be monitored for security and environmental conditions
- Eating, drinking, and smoking shall be prohibited in equipment rooms
- Unauthorized photography shall be prohibited in equipment rooms

5. Protection Against External and Environmental Threats

5.1 Environmental Controls

- Environmental controls shall be implemented based on risk
- Controls may include:
  - Temperature and humidity monitoring
  - Water leak detection
  - Fire detection and suppression
  - Uninterruptible power supplies
  - Backup power generators
  - Air conditioning redundancy
- Environmental conditions shall be monitored
- Environmental control systems shall be regularly maintained and tested
- Environmental incidents shall be promptly addressed

5.2 Natural Disaster Protection

- Facilities shall be protected against relevant natural disasters
- Protection measures shall be based on geographical location and risk
- Disaster response procedures shall be documented

- Staff shall be trained on disaster response
- Insurance coverage shall be maintained for natural disasters
- Recovery capabilities shall be established and tested

5.3 Malicious Threat Protection

- Facilities shall be protected against malicious threats
- Protection may include:
  - Intruder detection systems
  - CCTV surveillance
  - Security personnel
  - Reinforced construction
  - Blast-resistant measures (where appropriate)
- Threat intelligence shall inform protection measures
- Suspicious activity shall be reported and investigated
- Security incidents shall be documented and analyzed

6. Working in Secure Areas

6.1 Secure Area Procedures

- Procedures for working in secure areas shall be documented
- Procedures shall include:
  - Authorization requirements
  - Escort requirements
  - Recording of access
  - Behavior expectations
  - Prohibited activities
- Procedures shall be communicated to all relevant personnel
- Compliance with procedures shall be monitored
- Violations shall be addressed through appropriate channels

6.2 Supervision and Monitoring

- Secure areas shall be supervised as appropriate
- Unescorted access shall be limited to authorized personnel
- Video surveillance shall be implemented where appropriate
- Monitoring systems shall be regularly checked
- Monitoring records shall be retained according to policy
- Privacy considerations shall be addressed in monitoring activities

6.3 Delivery and Loading Areas

- Delivery areas shall be controlled and isolated from processing areas
- Delivery personnel shall not have access to secure areas
- Incoming materials shall be inspected before entering secure areas
- Incoming materials shall be registered upon entry
- Delivery areas shall be monitored by CCTV where appropriate
- Delivery procedures shall be documented and followed

7. Equipment Security

7.1 Equipment Siting and Protection

- Equipment shall be sited to minimize risks
- Equipment shall be protected from:
    - Environmental threats
    - Power failures
    - Unauthorized access
    - Theft or damage
    - Food and liquid spills
- Critical equipment shall have redundancy
- Equipment protection shall be regularly reviewed
- Equipment maintenance shall be performed regularly

7.2 Supporting Utilities

- Equipment shall be protected from power failures
- Uninterruptible power supplies shall be provided for critical equipment
- Emergency power off switches shall be available
- Multiple power feeds shall be considered for critical systems
- Power and telecommunications cabling shall be protected
- Supporting utilities shall be regularly inspected and tested
- Utility failures shall be monitored and addressed

7.3 Cabling Security

- Power and telecommunications cabling shall be protected
- Protection may include:
    - Conduits or cable trays
    - Avoiding routes through public areas
    - Separation from electrical interference
    - Physical access controls
    - Inspection for tampering or damage

- Cabling shall be clearly labeled
- Cabling documentation shall be maintained
- Unused cabling shall be removed

7.4 Equipment Maintenance

- Equipment shall be maintained according to manufacturer specifications
- Maintenance shall be performed by authorized personnel only
- Maintenance records shall be maintained
- Equipment containing sensitive data shall be supervised during maintenance
- Maintenance by external parties shall follow security requirements
- Equipment shall be inspected after maintenance

8. Asset Management

8.1 Equipment Asset Management

- Physical assets shall be identified and inventoried
- Asset ownership shall be assigned
- Asset classification shall be based on value and sensitivity
- Asset location shall be tracked
- Asset movement shall be authorized and documented
- Asset disposal shall follow secure procedures
- Asset inventory shall be regularly verified

8.2 Off-Premises Equipment

- Authorization shall be required for off-premises equipment
- Off-premises equipment shall be registered
- Security requirements shall apply to off-premises equipment
- Off-premises equipment shall be physically secured
- Insurance shall cover off-premises equipment
- Off-premises equipment shall be regularly verified
- Return of off-premises equipment shall be enforced

8.3 Secure Disposal or Reuse

- Equipment shall be verified for sensitive data before disposal
- Storage media shall be securely erased or destroyed
- Disposal shall be documented and verified
- Specialized disposal services shall be used where appropriate
- Equipment for reuse shall be sanitized of sensitive data
- Disposal shall comply with environmental regulations

- Certificates of destruction shall be obtained where appropriate

9. Physical Media Controls

9.1 Management of Removable Media

- Removable media shall be managed securely
- Removable media containing sensitive information shall be protected
- Removable media shall be stored in secure environments
- Removable media shall be logged and tracked
- Unauthorized media shall be prohibited in secure areas
- Media handling procedures shall be documented and followed

9.2 Media Disposal

- Media disposal procedures shall be documented
- Sensitive media shall be securely destroyed
- Destruction methods may include:
    - Shredding
    - Incineration
    - Degaussing
    - Physical destruction
- Media disposal shall be logged
- Disposal shall be verified
- Certificates of destruction shall be obtained where appropriate

9.3 Physical Media Transfer

- Media transfer procedures shall be documented
- Media shall be protected during transport
- Secure courier services shall be used where appropriate
- Media packaging shall protect against damage
- Chain of custody shall be maintained for sensitive media
- Media transfer shall be logged and tracked
- Recipients shall acknowledge receipt of media

10. Mobile Device Physical Security

10.1 Mobile Device Protection

- Mobile devices shall be physically secured
- Devices shall not be left unattended in public places
- Screen locks shall be enabled

- Devices shall be carried securely during travel
- Theft-deterrent measures shall be implemented where possible
- Lost or stolen devices shall be reported immediately
- Remote wipe capabilities shall be enabled where possible

10.2 Travel Security

- Travel security guidelines shall be provided to staff
- Guidelines shall address:
    - Physical protection of devices
    - Observation of surroundings
    - Secure use in public places
    - Border crossing considerations
    - Hotel security practices
- High-risk travel shall have additional security measures
- Travel incidents shall be reported and analyzed

11. Physical Security Monitoring

11.1 Security Monitoring Systems

- Physical security monitoring systems shall be implemented
- Systems may include:
    - CCTV surveillance
    - Intruder detection
    - Access control monitoring
    - Environmental monitoring
- Monitoring systems shall be regularly tested
- Monitoring data shall be protected
- Monitoring shall comply with privacy regulations

11.2 Alarm Response

- Alarm response procedures shall be documented
- Alarms shall be promptly investigated
- Response personnel shall be trained
- False alarms shall be analyzed and addressed
- Alarm systems shall be regularly tested
- Alarm response shall be documented
- Alarm systems shall have backup power

12. Roles and Responsibilities

12.1 Facilities Management

- Implement physical security controls
- Maintain physical security systems
- Coordinate with security personnel
- Manage environmental controls
- Respond to physical security incidents
- Maintain facility documentation

12.2 Information Security Team

- Define physical security requirements
- Assess physical security risks
- Review physical security incidents
- Provide physical security guidance
- Coordinate with facilities management
- Ensure compliance with standards

12.3 Department Managers

- Ensure staff compliance with physical security policies
- Report physical security concerns
- Authorize access for their staff
- Support physical security awareness
- Participate in physical security assessments
- Implement department-specific controls

12.4 All Personnel

- Follow physical security procedures
- Report security incidents and concerns
- Protect assigned access credentials and keys
- Challenge unauthorized individuals
- Maintain clean desk practices
- Participate in security awareness training

13. Compliance and Exceptions

13.1 Compliance Monitoring

- Physical security compliance shall be regularly assessed

- Assessments may include:
    - Physical security audits
    - Penetration testing
    - Access control reviews
    - CCTV footage reviews
- Non-compliance shall be addressed through appropriate channels
- Compliance trends shall be analyzed and reported

13.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

14. Related Documents

- Information Security Policy
- Asset Management Policy
- Clear Desk and Clear Screen Policy
- Data Protection Policy
- Business Continuity Plan
- Visitor Management Procedure
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

15. Approval

This Physical Security Policy is approved by:

Name: ________________________ Position: ______________________ Date: _________________________ Signature: _____________________