Physical and Environmental Security Policy Template

Document Control Information

- **Document Title:** Physical and Environmental 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 and Environmental Security Policy establishes [ORGANIZATION NAME]'s requirements for protecting facilities, equipment, and information assets from physical and environmental threats in accordance with ISO 27001:2022 requirements. It provides a framework for implementing and maintaining physical security controls to prevent unauthorized physical access, damage, theft, compromise, or interference.

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 and environmental 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 and environmental security measures - Complying with relevant legal, regulatory, and contractual requirements - Regularly reviewing and improving physical and environmental 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. Off-Premises Equipment Security

8.1 Mobile Device Security

- Mobile devices shall be physically secured
- Security measures may include:
  - Cable locks
  - Security cases
  - Tracking software
  - Remote wipe capabilities
- Mobile devices shall not be left unattended in public places
- Mobile device security shall follow the Mobile Device Policy
- Mobile device loss or theft shall be promptly reported
- Mobile device security shall be regularly assessed

8.2 Teleworking Security

- Teleworking environments shall be physically secured
- Security measures may include:
  - Secure storage
  - Screen privacy filters
  - Cable locks
  - Access controls
- Teleworking security shall follow the Remote Working Policy
- Teleworking security shall be regularly assessed
- Teleworking security incidents shall be promptly reported
- Teleworking security guidance shall be provided to staff

8.3 Off-Site Equipment

- Off-site equipment shall be physically secured
- Security measures shall be appropriate to location risk
- Off-site equipment shall be registered and tracked
- Off-site equipment shall be regularly verified
- Off-site equipment security shall be regularly assessed
- Off-site equipment security incidents shall be promptly reported
- Off-site equipment security guidance shall be provided to staff

9. Secure Disposal and Reuse

9.1 Equipment Disposal

- Equipment disposal shall follow secure procedures
- Procedures shall include:
  - Data sanitization
  - Physical destruction where appropriate
  - Disposal documentation
  - Chain of custody
- Disposal shall be performed by authorized personnel
- Disposal shall be verified
- Disposal shall comply with environmental regulations
- Disposal procedures shall be regularly reviewed

9.2 Media Disposal

- Media disposal shall follow secure procedures
- Procedures shall be appropriate to media type and sensitivity
- Methods may include:
  - Secure deletion
  - Degaussing
  - Physical destruction
  - Shredding
- Disposal shall be performed by authorized personnel
- Disposal shall be verified
- Disposal shall be documented
- Disposal procedures shall be regularly reviewed

9.3 Equipment Reuse

- Equipment reuse shall follow secure procedures

- Procedures shall include:
    - Data sanitization
    - Software removal
    - Configuration reset
    - Verification
- Reuse shall be performed by authorized personnel
- Reuse shall be documented
- Reuse shall be verified
- Reuse procedures shall be regularly reviewed

10. Physical Security Monitoring

10.1 CCTV Surveillance

- CCTV systems shall be implemented where appropriate
- CCTV coverage shall include:
    - Entry and exit points
    - Secure areas
    - Perimeters
    - High-value asset locations
- CCTV footage shall be retained according to policy
- CCTV systems shall be regularly maintained and tested
- CCTV monitoring shall respect privacy requirements
- CCTV usage shall be clearly communicated

10.2 Alarm Systems

- Alarm systems shall be implemented where appropriate
- Alarm types may include:
    - Intruder detection
    - Fire detection
    - Environmental monitoring
    - Access control violations
- Alarms shall be monitored continuously
- Alarm response procedures shall be documented
- Alarm systems shall be regularly maintained and tested
- False alarms shall be investigated and addressed

10.3 Security Personnel

- Security personnel shall be deployed where appropriate
- Personnel shall be properly trained and qualified
- Personnel shall follow documented procedures

- Personnel shall maintain logs and reports
- Personnel shall respond to security incidents
- Personnel performance shall be regularly assessed
- Personnel shall coordinate with other security measures
- Personnel shall receive regular security updates

11. Environmental Security

11.1 Fire Protection

- Fire protection systems shall be implemented
- Systems shall include:
  - Fire detection
  - Fire suppression
  - Fire alarms
  - Evacuation routes and signage
- Systems shall comply with local regulations
- Systems shall be regularly maintained and tested
- Staff shall be trained on fire procedures
- Fire incidents shall be documented and analyzed
- Fire protection shall be regularly assessed

11.2 Water Protection

- Water damage protection shall be implemented
- Protection may include:
  - Leak detection
  - Drainage systems
  - Raised floors
  - Waterproof covers
  - Water-resistant construction
- Critical areas shall have enhanced protection
- Water incidents shall be promptly addressed
- Water protection shall be regularly assessed
- Water protection shall be regularly tested

11.3 Temperature and Humidity Control

- Temperature and humidity shall be controlled in sensitive areas
- Controls shall be appropriate to equipment requirements
- Monitoring systems shall be implemented
- Alerts shall be configured for out-of-range conditions
- Control systems shall be regularly maintained

- Backup systems shall be available for critical areas
- Temperature and humidity incidents shall be promptly addressed
- Control effectiveness shall be regularly assessed

11.4 Power Management

- Power management systems shall be implemented
- Systems shall include:
  - Uninterruptible power supplies (UPS)
  - Backup generators
  - Power conditioning
  - Surge protection
- Critical systems shall have redundant power
- Power systems shall be regularly maintained and tested
- Power incidents shall be promptly addressed
- Power management shall be regularly assessed

12. Physical Security in the System Lifecycle

12.1 Physical Security Planning

- Physical security shall be considered in system planning
- Planning shall include:
  - Location selection
  - Space requirements
  - Environmental requirements
  - Security requirements
  - Growth considerations
- Planning shall involve relevant stakeholders
- Planning shall be documented
- Planning shall be regularly reviewed
- Planning shall align with organizational strategy

12.2 Physical Security Implementation

- Physical security shall be implemented during system deployment
- Implementation shall follow documented plans
- Implementation shall be verified against requirements
- Implementation shall be documented
- Implementation shall be approved before operation
- Implementation shall be regularly assessed
- Implementation shall be updated as needed

12.3 Physical Security Decommissioning

- Physical security shall be considered in system decommissioning
- Decommissioning shall include:
  - Secure removal of equipment
  - Secure disposal of media
  - Access control updates
  - Documentation updates
  - Physical security reassessment
- Decommissioning shall be documented
- Decommissioning shall be verified
- Decommissioning shall be approved
- Decommissioning shall follow secure procedures

13. Roles and Responsibilities

13.1 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
- Report on physical security status

13.2 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
- Report on security status

13.3 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
- Report on departmental security status

13.4 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
- Support physical security initiatives

14. Compliance and Exceptions

14.1 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
- Compliance reports shall be provided to management
- Compliance monitoring shall be regularly reviewed

14.2 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 - Tracked and reported - Minimized to the extent possible - Consistent with legal and regulatory requirements

15. 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]

16. Approval

This Physical and Environmental Security Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____