# Physical and Environmental Security Policy

Version [Revision #]

Last modified: [Last modified date]

Last reviewed: [Last reviewed date]

Last Approval: [Last approval date]

#### *Disclaimer*

*This policy template is created as a useful resource. However, organizations remain fully responsible for the content of their policies. Every organization is unique, and the content and format of this template must be revised to meet your organization’s specific requirements. The set of templates available from Hyperproof is not exhaustive nor inclusive; your organization may choose to use only a portion of them or to split them into multiple policies. Do not rely on this policy template to meet legal, regulatory, or contractual requirements. Review your policy in detail to ensure that it is appropriately tailored to your organization's business objectives and legal requirements.*

### Security boundary under scope

1. [List of applicable systems]

### References

1. ISO/IEC 27001:2022: A.7.1, A.7.5, A.7.8, A.7.11, A.7.12, A.7.13
2. NIST 800-53 rev. 5: CM-7, MA-1, MA-3, MA-3(1), MA-3(2), MA-3(3), MA-4, MA-5, MA-5(1), MA-6, MP-2, MP-4, MP-7, PE-1, PE-2, PE-3, PE-4, PE-9, PE-11, PE-12, PE-13, PE-13(1), PE-13(2), PE-14, PE-15, PE-16, PE-17
3. PCI DSS 4.0: 9.1.1, 9.2.1, 9.3.1, 9.3.1.1, 9.4.1
4. AICPA SOC 2 TSC: A1.2, C1.1, CC5.1, CC5.2, CC6.4, CC7.1, CC7.2

## Document ownership

 <(Choose from)>

* 1. Policy Owner:
		1. [Owner name] ([Owner email]), [Owner title]
	2. Information Security Officer:
		1. [Information officer name], ([Information officer email]), [Information officer title]
	3. System Owner(s):
		1. [System owner name], ([System owner email]), [System owner title]
	4. Process and Operational Owner(s)
		1. [process owner], ([process owner email]), [process owner title]
	5. System Administrator(s):
		1. [System admin name], ([System admin email]), [System admin title]
	6. Required Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT
	7. Optional Dissemination: <(Choose from)>
		1. IT Administrator
		2. Engineering
		3. Product Management
		4. Support
		5. Information Security Team
		6. [Organization name] Leadership Team
		7. Contractors
		8. Vendors
		9. Company Wide
		10. [Organization name] SIRT

## Purpose

The purpose of the Physical and Environmental Security Policy is to establish a framework for safeguarding the organization's physical infrastructure, critical equipment, and protected information. This policy aims to mitigate risks associated with physical threats, unauthorized access, environmental hazards, and other potential disruptions that could impact the confidentiality, integrity, and availability of the organization's information systems. By implementing physical and environmental controls, the organization ensures the continued operation and security of its critical assets and supports the overall information security objectives.

## Scope

This policy applies to all facilities, physical components, and areas housing information systems within the organization, including but not limited to data centers, server rooms, office spaces, and other secure locations. The policy covers:

* Physical security strategy
* Safe and secure equipment installation and monitoring
* Physical access control
* Visitor access management
* Water damage protection
* Fire detection and suppression
* Temperature and humidity management
* Physical ethernet port protection
* Power resilience and safety (UPS, generators, emergency shutoff, emergency lighting)
* Cable security

All employees, contractors, vendors, and visitors with access to the organization's facilities are required to comply with this policy. The primary focus is on protecting critical equipment, protected information, and secure areas, ensuring that all physical and environmental security measures align with industry best practices and regulatory requirements.

## Roles and responsibilities

<(choose from)>

| **Role** | **Person &/or Title** | **Responsibility** |
| --- | --- | --- |
| Plan and Policy Management | [Owner name], [owner title] | Establish the controls, implementation, and monitoring strategy for [policy topic] and associated policy and procedure |
| Executive Review | Executive Team | Adjusts [policy topic] parameters to meet business requirements and appropriate risk appetite. Approves risk model and supporting risk documentation that applies to the [policy topic] Policy. Reads, understands and approves after appropriate editing, the [policy topic] Policy. |
| Approval and Commitment | Executive Team | Responsible for approval, and commitment to information security controls. Members of the leadership team of [Organization] to include [list of executive approvers]. |
| Information System Owner | [Information officer name], [Information officer title] | Responsible for the overall implementation, development, integration, modification, or operation and maintenance of configuration management. Develops operational strategies and tactics to comply with configuration management policy in coordination with the information systems administrators, the information security officer, and functional “end users.” |
| Operations | [Operational owner], Operational owner title] |  |
| Information Systems Administrators | System Administrators  | Effectively manages the daily implementation, monitoring, and maintenance of operational security controls, as directed by the System Owner and Information Security Officer. |
| Human Resource | [HR name], [HR title] | Setups HR wellbeing strategies, coordinates travel policy across the organization. Initiates emergency travel considerations, including crisis management when required. |
| End Users |  End Users | Users of information systems are required to comply with policy and procedures in the [policy topic] policy. |
| Providers | [provider type] | [provider service description] |

## Management commitment

* 1. [Organization] executive management affirms its commitment to the establishment, implementation, resourcing, monitoring, and effectiveness of [policy topic] controls and policy
	2. Management has reviewed and approved this policy.
	3. This policy demonstrates management's commitment to maintaining adequate controls as part of its information security management and privacy objectives. These objectives include compliance with applicable laws, regulatory requirements, executive orders, industry best practices, standards, guidelines, and contractual commitments.
	4. Management agrees to regularly review and update this policy to ensure that it effectively meets the organization’s business and compliance objectives.

## Coordination among organizational entities

1. The [responsible group] creates policy and procedure and is responsible for overall configuration management.
2. Policy and procedures will be reviewed, modified, and disseminated to required consumers.
3. The [responsible group] is responsible for coordinating documentation review and updating the policy.
4. The [responsible group] is responsible for communicating the policy and procedures to applicable required and optional parties.
5. The [responsible group] is responsible for training applicable required and optional parties on compliance with the policy and procedures.

## Compliance

* 1. Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties.
	2. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties

## Definitions

* 1. Access Control: Mechanisms that restrict entry to physical locations or access to information systems to authorized personnel only.
	2. Biometric Scanner: A security device that uses individuals' unique biological characteristics, such as fingerprints or retinal patterns, for identification and access control.
	3. Critical Equipment: Hardware and devices essential to the organization's information systems and operations, whose failure would significantly impact the organization's functionality.
	4. Environmental Monitoring: The continuous observation and recording of environmental conditions such as temperature, humidity, and air quality to ensure they remain within safe parameters for equipment operation.
	5. HVAC Systems: Heating, Ventilation, and Air Conditioning systems used to regulate and maintain the temperature and humidity levels within a facility.
	6. Physical Security: Measures designed to protect physical facilities, equipment, and personnel from harm, theft, or unauthorized access.
	7. Secure Area: A designated zone within a facility that has implemented enhanced security measures to protect critical assets and sensitive information.
	8. Uninterruptible Power Supply (UPS): A backup power system that provides emergency power to critical equipment in the event of a power failure, ensuring continued operation.
	9. Visitor Management System: A process or system used to register, badge, and track visitors within a facility to ensure their activities are monitored and controlled.
	10. Water Detection System: A system designed to detect the presence of water or leaks, typically used in areas where water intrusion could damage critical equipment.
	11. Emergency Shutoff: Mechanisms or systems that allow for the immediate discontinuation of power or other utilities in an emergency to protect personnel and equipment.
	12. Port-Based Network Access Control (NAC): Security measures that control access to the network through specific ports, ensuring only authorized devices can connect.
	13. Cable Management Systems: Structures and practices used to organize, secure, and protect electrical and data cables within a facility.
	14. Fire Detection and Suppression Systems: Systems designed to detect the presence of fire and automatically initiate measures to extinguish or control it, such as alarms, smoke detectors, and sprinklers.
	15. Power Resilience: The capability of a facility to maintain continuous power supply to critical equipment through UPS, generators, and other backup systems during power outages.

## Policy

#### Physical Security Strategy

The [responsible party] shall:

* + 1. Develop and implement a physical security strategy that includes risk assessment, mitigation measures, and periodic reviews to ensure the protection of critical equipment, protected information, and secure areas.
		2. Define and designate secure areas with specific security requirements based on the criticality of the information and equipment contained within.
		3. Install all equipment securely in designated areas, ensuring they are physically stable and protected from unauthorized access.

#### Physical Access Control

The [responsible party] shall:

* + 1. Implement physical access controls to limit access to secure areas to authorized personnel only, using methods such as key cards, biometric scanners, and security personnel.
		2. Maintain access logs and periodically review them to detect and respond to unauthorized access attempts.
		3. Establish a visitor management system that includes visitor registration, issuance of visitor badges, and escort requirements.
		4. Maintain visitor logs for a minimum period as defined by organizational policies and conduct regular reviews to ensure compliance.

#### Water Damage Protection

The [responsible party] shall:

* + 1. Implement measures to protect against water damage, such as water detection systems, waterproof enclosures for critical equipment, and regular inspections of plumbing and drainage systems.
		2. Ensure proper maintenance of facilities to prevent leaks and water intrusion.

#### Fire Detection and Suppression

The [responsible party] is required to:

* + 1. Install and maintain fire detection and suppression systems in accordance with local regulations and industry standards, including smoke detectors, fire alarms, and automatic sprinkler systems.

#### Temperature and Humidity Management

The [responsible party] is required to:

* + 1. Maintain temperature and humidity levels within the manufacturer-specified ranges for all critical equipment
		2. Plan and properly install equipment to optimize airflow
		3. Regularly inspect and maintain temperature and humidity control systems to ensure they function correctly and efficiently.
		4. Continuously monitor environmental conditions such as temperature, humidity, and air quality in areas housing critical equipment.
		5. Implement alert systems to notify relevant personnel of any deviations from established environmental parameters.

#### Physical Ethernet Port Protection

The [responsible party] shall:

* + 1. Secure physical ethernet ports by disabling unused ports and using port security measures such as port-based Network Access Control (NAC).
		2. Conduct periodic audits of active ethernet ports to ensure compliance with security policies.

#### Power Resilience and Safety

The [responsible party] is required to:

* + 1. Implement uninterruptible power supplies (UPS) and backup generators to ensure continuous power to critical equipment during power outages.
		2. Ensure emergency power shutoff mechanisms are in place and easily accessible.
		3. Install emergency lighting in all critical areas to provide visibility during power failures.
		4. Conduct regular testing and maintenance of all power resilience equipment.

#### Cable Security

The [responsible party] shall:

* + 1. Implement measures to protect cables from physical damage and unauthorized access, including the use of cable management systems and secure conduits.
		2. Regularly inspect and maintain cable integrity and security to prevent data loss or breaches.

## Policy exemptions

* 1. Requests for exceptions to this policy shall be reviewed by the [exemption officer 1] and the [exemption officer 2] and/or the [responsible group].
	2. Employees requesting exceptions shall provide such requests to [exemption communication channel].
	3. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the [responsible group], initiatives, actions, and a timeframe for achieving the minimum compliance level with the policies set forth herein.

## Related documents

* 1. [list of related documents, including:
		1. Policies
		2. Procedures
		3. Standards
		4. Documentation
		5. Regulations
		6. Legal context

]

## Revision history

* 1. This policy is reviewed and, if necessary, updated annually and may also be updated to reflect changes in the environment.
	2. Every change to this plan must be reviewed and evidence of review and acceptance noted with a signature below. This plan requires the signature of: <(choose from)>
		1. The Information Security Officer
		2. Officer of the [Organization name] Leadership Team
	3. All changes requiring approval must be communicated to the required parties

| **Rev. #** | **Revision Date** | **Description** | **Author** | **Owner** | **Exec. reviewer** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

## Approval history

| **Step** | **Approver** | **Job Function** | **Signature** | **Approval Date** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |