Physical and Environment Security Policy

Information Security

Version 1.0

Prepared By:
Hrushikesh Mehendale

Reviewed By:
Shruti Deshpande

FlaggGRC

Document Control

Last Modified	Reason For Change	Suggested By	Approved By
6 April 2025	Document created	Hrushi M	Shruti D
25 Mar 2026	Document reviewed, no change	Hrushi M	Shruti D
7 Oct 2026	Document reviewed, no change	Hrushi M	Shruti D

Purpose

The purpose of this policy shall be to establish guidelines for physically securing the company office premises.

Scope

All staff users. Company office.

Principle

Physical assets in the company office premises shall be secured according to their risk levels.

Physical Assets

The information regarding physical assets shall be maintained in the Physical Assets Register. Physical assets covered under the scope shall be:

- Laptops
- Mobile phones
- Networking equipment
- Physical copies of agreements

📓 Physical Assets Register

Physical Security Perimeter

The physical security perimeter shall encompass all physical boundaries that define and protect the company's office space. It shall include the following:

- **Boundaries:** The structural elements that enclose the office space, including the ceiling, walls, and flooring, which shall ensure a secure and enclosed environment.
- **Entry Points:** All designated access areas, such as doors and windows, which shall serve as controlled entry and exit points for authorized personnel.
- **Secure Areas:** Specific office zones that shall house critical operations, sensitive information, or restricted activities, ensuring controlled access based on authorization levels.
- **Secure Storage Areas:** Dedicated spaces such as server rooms, file storage units, or locked cabinets, which shall be used to store sensitive documents, equipment, or digital assets securely.
- **Workspace Areas:** General office areas where employees shall perform their daily tasks, designed to balance accessibility with security measures.
- **Network Areas:** Sections of the office containing network infrastructure, including server racks, networking devices, and structured cabling, which shall be protected to ensure data security and operational continuity.

These elements shall collectively form a well-defined perimeter, ensuring a secure and controlled working environment.

FlagGRC

Ceiling, Walls, and Flooring

- The structural integrity of the ceilings, walls, and flooring shall be assessed and maintained to prevent unauthorized entry.
- Materials used for construction shall be durable and resistant to physical penetration.

Doors

- The door shall be sturdy with a biometric lock facility.
- An additional protective door with a lock and key shall be provided.
- Staff and visitor entry shall be monitored.
- Entry shall be monitored via CCTV.

Windows

- Window panes shall have a locking mechanism and be in good condition.
- Windows shall have an exterior protective metallic grill.

Secure Areas

- Secure areas shall be demarcated with clear signage.
- Secure areas shall have a door or a partition to separate it from the rest of the office space.
- Only management representatives shall be allowed to work in secure areas.
- Entry in secure areas shall require authorization from management.
- Entry shall be monitored via CCTV.

FlagGRC

Administrative Areas

- Administrative areas shall be demarcated with clear signage.
- Only human resource representatives, admin representatives and management representatives shall be allowed to work in administrative areas.
- Entry in administrative areas shall require authorization from management.

Secure Storage Areas

- Areas used for storing sensitive information or assets shall be physically secure
- Secure storage areas shall be demarcated with clear signage.
- A tamper proof locking mechanism shall be installed.

- The key to the storage shall be given to the admin person only.
- Entry shall be monitored via CCTV.

Networking Areas

- All areas housing network infrastructure (e.g., server rooms, networking closets) shall be physically secured with robust access controls.
- Networking areas shall be demarcated with clear signage.
- Networking areas shall be installed away from easy access.
- They shall be physically secured with lock and key, key shall remain with the admin person only.

Workspace Areas

- Workspace areas where staff members work shall be made comfortable for working
- The area shall be demarcated with clear signage.
- The area shall be restricted to staff members only.

Office Keys

Types of Physical Keys Used for Securing the Physical Premises

To ensure the safety and integrity of the organization's physical infrastructure, the following types of keys shall be utilized for controlled access and security purposes:

- Exterior Protective Door Keys
  - These keys are designated for the primary external access points of the facility. They are intended to secure the perimeter entryway.
- Entry Door Biometric Lock Backup Keys
  - These are physical backup keys associated with doors that are primarily secured using biometric access control systems. In the event of biometric system failure or maintenance requirements, these keys may be used to allow authorized entry.
- Secure Storage Keys
  - These keys are assigned to secure areas containing confidential information, equipment, or assets.
- Network Area Keys
  - These keys provide access to areas housing critical IT infrastructure, such as server rooms, network racks, and communications equipment.

Access to Physical Keys

FlaggGRC

Keys	All Staff	Admin Rep	Management Rep
Exterior Protective Door Keys	Keys provided	Keys provided	Keys provided
Entry Door Biometric Lock Backup Keys	No access	Keys provided	Keys provided
Secure Storage Keys	No access	Keys provided	Keys provided
Network Area Keys	No access	Keys provided	Keys provided

📓Office Key Register
📓Visitor Register
📓Secure Storage Register
📓Signage Register

Environmental Issues

Identification of Issues

The following environmental issues shall be considered significant within the scope of the ISMS, as they may pose risks to the confidentiality, integrity, and availability of information assets:

- Physical Intrusions:
  - Unauthorized access to premises or information systems that may lead to data breaches or compromise of critical assets.
- Theft & Vandalism:
  - Theft of equipment or deliberate damage to physical or digital infrastructure, potentially resulting in data loss or service disruption.
- Floods:
  - Water damage from natural disasters or plumbing failures that could impact hardware, documents, or facility operations.
- Fires:
  - Fire incidents that may destroy physical infrastructure, hardware, or records, leading to severe operational and data loss.
- Earthquakes:
  - Seismic events that can damage buildings, communication lines, and data centers, disrupting business continuity.
- Climate Variations:
  - Extreme weather conditions (e.g., heatwaves, storms) that could affect the reliability of IT infrastructure or working conditions.

FlaggGRC

- Civil Unrest:
    - Social or political disturbances that may threaten physical security, limit access to facilities, or impact staff safety.
- Cyber Attacks on Premises:
    - Targeted attacks on internal networks or systems housed within physical premises, including unauthorized network access, malware, or ransomware affecting onsite infrastructure.

Identification & Mitigation of Risks

For each environmental issue, risks shall be identified and mitigating controls shall be put in place. These risks shall also be considered while doing the organization-wide risk assessment via the Risk Register.

Issue	Risks	Risk Mitigation Plan
Physical Intrusions	Loss of access to data Loss of data Data leak/misuse Data corruption	• Store as less data as possible in office • Avoid storing sensitive data in office • Backup the data on cloud • Ensure doors and window panes are equipped with tamper-proof locking mechanisms wherever possible and seal securely when closed.
Theft & Vandalism	Loss of access to data Loss of data Data leak/misuse Data corruption	• Store as less data as possible in office • Minimize the presence of unused and unnecessary data storage and processing devices in the office. • Avoid storing sensitive data in office • Backup the data on cloud • Ensure doors and window panes are equipped with tamper-proof locking mechanisms wherever possible and seal securely when closed.
Floods	Loss of access to data Loss of data Threat to employee safety	• Avoid taking up office space at the ground level • Store as less data as possible in office
Fires	Loss of access to data Loss of data Threat to employee safety	• Avoid using heavy electricals and machinery in office • Avoid kitchen activities in office such as cooking with gas

FlaggGRC

		• Avoid using inflammable material and substances as much as possible • Minimize the usage, storage and flow of paper in business activities
Earthquakes	Loss of access to data Loss of data Threat to employee safety	• Acquire office space in premises that has good construction quality • To facilitate easy escape in earthquake situations, take up the office space on the first floor
Climate Variations	Loss of access to data Loss of data Threat to employee safety	• Acquire office space in premises that has good construction quality • Ensure doors and window panes are equipped with locking mechanisms and seal securely when closed.
Civil Unrest	Loss of access to data Threat to employee safety	• Acquire office space in premises that has good construction quality • Ensure doors and window panes are equipped with locking mechanisms and seal securely when closed. • Backup the data on cloud
Cyber Attacks on Premises	Loss of access to data Loss of data Data Leak/Misuse Data corruption	• Store as less data as possible in office • Avoid storing sensitive data in office • Backup the data on cloud

📓 Risk Register

FlaggGRC

Assets Off-Premise

Assets shall never be kept off-premise on a permanent basis. Assets shall be taken off-premise on a temporary basis in the following scenarios:

Asset	**Off-premise Scenarios**
Laptops	• Staff members visit client or vendor locations • Staff members work from home • Staff members are travelling
Mobile Phones	• Staff members visit client or vendor locations

	• Staff members work from home • Staff members are travelling

Staff members who take company assets off-site shall adhere to the following requirements to ensure the security and proper handling of information assets:

- Adherence to Remote Working Policy:
  - Staff shall comply with all provisions outlined in the company's remote working policy, including restrictions on location and permitted activities.
- Endpoint Security:
  - Staff shall ensure that endpoint security measures, such as firewalls, encryption, and secure login credentials, are properly configured and active on their devices.
- Clear Desk and Clear Screen Policy:
  - Staff shall follow the company's clear desk and clear screen policy at all times, ensuring sensitive information is not left exposed or unattended.
- Antivirus and Anti-Malware Protection:
  - Staff shall ensure that approved antivirus and anti-malware software is installed, up to date, and actively running on any device used to access company systems or data.

Utility Services

Following are the utility services of significance from the scope of the ISMS:

- Power supply
- Breadband internet

These shall be managed via the Third Party Register.

📓 Third Party Register

FlaggGRC

Cabling Security

Scope of Cabling Security

The scope shall include the following cabling in the company office:

- Power cabling
- Broadband internet cabling

Power Cabling

This shall cover all electrical cabling used to supply power to workstations, network devices, and other equipment.

Following are the risks associated with power cabling:

- Physical damage to cabling
- Rodent damage
- Overheating
- Overloading
- Moisture exposure

Following are the mitigation measures to ensure the risks stay within acceptable limits:

- Avoiding physical damage:
  - Avoid cabling on floors
  - Avoid dangling cables
  - Use trays and organizers
- Avoiding overheating:
  - Use high quality cables sufficient for the expected load
  - Avoid using high voltage equipment
- Avoiding moisture exposure:
  - Keep cables away from water sources and high-moisture areas to prevent electrical shorts and corrosion.
- Avoiding overloading:
  - Use surge protectors and circuit breakers to guard against overloads and power surges.
- Avoiding rodent damage:
  - Avoid cabling in areas where rodents might be present

Broadband Internet Cabling

This shall include all data cabling used to provide internet connectivity, including structured LAN cabling, modem/router connections, and any associated wiring that supports network access.

Following are the risks associated with power cabling:

- Physical damage to cabling
- Signal degradation
- Cable cyberattack

Following are the mitigation measures to ensure the risks stay within acceptable limits:

- Physical damage:
  - Place the cable-related equipment in a secure cabinet.
- Signal degradation:

FlaggGRC

    - Conduct regular inspections to check the signal quality
- Cybersecurity:
    - Control physical access to the equipment
    - Ensure that data transmitted over the cable is encrypted.

Equipment Maintenance

Regular maintenance shall be conducted on the following equipment:

- Fire extinguisher
- Printer

Maintenance will be conducted on an annual basis.

Monitoring

To ensure the protection of information assets and compliance with the organization's security policies, monitoring of physical security shall fall under two key categories:

- Continuous Monitoring
    - This includes real-time surveillance and security controls that operate on an ongoing basis.
    - Examples include CCTV surveillance, access control systems (such as biometric or keycard entry).
    - The purpose of continuous monitoring is to detect and respond to unauthorized access or suspicious activity immediately.
- Periodic Monitoring
    - This involves scheduled reviews and assessments of physical security measures.
    - Examples include physical security audits, access log reviews, equipment inspections, and compliance checks against physical security policies.
    - Periodic monitoring helps identify potential vulnerabilities, ensure proper functioning of security systems, and verify adherence to security protocols over time.
    - Periodic monitoring shall be conducted once in six months.

FlaggGRC

Policy Compliance

Exceptions

Any exception to this policy shall be approved and recorded by the CISO in advance and reported to the Management Review Team.

Non-Compliance

Any staff found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.

Continual Improvement

This policy is updated and reviewed as part of the continual improvement process.

FlaggGRC