[Company]

PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Security of physical locations and environments

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Physical and Environmental Security Policy

3.1 Purpose

The purpose of the policy is to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

3.2 Scope

All company owned or leased premises or locations deemed in scope by the ISO 27001 scope statement. Our of scope is third party and supplier physical and environmental security.

All employees and third-party users.

3.3 Principle

Physical and environmental security policy is built on the principle of exceeding Health and Safety regulation whilst protecting the most sensitive physical assets based on risk.

3.4 Physical Security Perimeter

The physical perimeter of the building or site containing information processing facilities is physically sound. The exterior roof, walls and flooring of the site are of solid construction and all external doors are suitably protected against unauthorized access with control mechanisms (list them – for example: bars, alarms, locks, enter-cards).

Doors and windows are locked when unattended and external protection in the form of bars is in place for windows, particularly at ground level.

Access to sites and buildings is restricted to authorised personnel.

A manned reception area grants access to the building and maintains a record of access.

All fire doors on a security perimeter are alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national, and international standards. They should operate in accordance with the local fire code in a failsafe manner.

Suitable intruder detection systems are installed to national, regional, or international standards.

Information processing facilities managed by the organization are physically separated from those managed by external parties.

3.5 Secure Areas

Access rights to secure areas are regularly reviewed and updated and revoked when necessary.

Access to secure areas defaults to deny.

Access to areas where confidential information is processed or stored is restricted to authorized individuals only by implementing appropriate access controls, (list them - example: by implementing a two-factor authentication mechanism such as an access card and secret PIN).

Logs of access are held and maintained for a minimum of 3 months.

External third-party support service personnel are granted restricted access to secure areas or confidential information processing facilities only when required and always accompanied; this access is authorized and monitored.

Photographic, video, audio, or other recording equipment, such as cameras in mobile devices is not permitted in secure areas unless authorized.

3.6 Employee Access

Employee access is based on least privilege providing access based on role.

Access control tokens, badges, are allocated to identify the employee or personnel and must be always worn.

Access control tokens, badges, are not shared, transferred, or loaned.

Access is revoked immediately upon termination and all physical access tokens are disabled and must be returned.

3.7 Visitor Access

Visitors are allowed unfettered access to the public areas.

Visitors are issued with instructions on the security requirements of the area and on emergency procedures.

Visitors are recorded in the visitor logbook and the information maintained for a minimum of 3 months.

Visitors are allocated a visitor pass that clearly identifies the visitor status, denies access to secure areas, and expires at the end of the business day on which issued.

Visitor access to secure areas requires verification of identity and presenting photographic identification.

Visitors are always escorted, except in the use of public areas and bathrooms.

3.8 Delivery and Loading Areas

Access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel.

The delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building.

The external doors of a delivery and loading area should be secured when the internal doors are opened,

Incoming material should be inspected and examined for explosives, chemicals, or other hazardous materials, before it is moved from a delivery and loading area.

Incoming material should be registered in accordance with asset management procedures on entry to the site.

Incoming and outgoing shipments should be physically segregated, where possible.

Incoming material should be inspected for evidence of tampering on route. If such tampering is discovered, it should be immediately reported to security personnel.

3.9 Network Access Control

Physical access to networking equipment is restricted which includes wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

Network jacks / points in public areas do not allow access to the company internal network.

Network jacks / points that allow access to the company internal network are secured by physical access control for entry and exit.

Visitors are prohibited from connecting devices to network jacks / points that allow access to the company internal network unless explicitly authorised to do so and are always escorted in areas with active network jacks / points.

3.10 Cabling Security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference, or damage.

Power and telecommunication lines into processing facilities are underground.

Power cables are segregated from communication cables to prevent interference.

Physical access to network cables is restricted where possible.

Access to cable rooms and patch panels is restricted by physical access control.

3.11 Equipment Siting and Protection

Equipment should be sited to minimize unnecessary access into work areas.

Information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use.

Storage facilities should be secured to avoid unauthorized access.

Items requiring special protection should be safeguarded to reduce the general level of protection required.

Controls should be adopted to minimize the risk of potential physical and environmental threats, e.g., theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism.

Guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established.

Environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.

Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines.

The use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments.

Equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

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