AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

This document details the physical and environmental security to prevent unauthorised physical access, damage and interference to the organisation's information and other associated assets.

SCOPE

This control applies to physical areas within the organization.

REFERENCE

ISO/IEC 27001 Standard	Annex A 7 Physical controls

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

The Management Representative (MR) shall ensure that the controls here are implemented.

PROCEDURES

1. Physical Security Perimeters

The organization operates within a co-working facility but maintains a dedicated, lockable private office unit. Access to this unit is restricted and secured, with keys issued only to authorized employees.

While the co-working space provides general building-level security (e.g., reception, CCTV, card-based controlled entry), the organization retains responsibility for securing its dedicated office unit and any sensitive information stored within.

2. Physical Entry

Access to the building is controlled by the co-working space provider through a card-based access control system. Within the building, the organization maintains a dedicated, lockable office unit, secured by a physical key. Keys are issued only to authorized employees and are promptly revoked upon termination or change in role requiring restricted access.

All alternative entry points, such as windows and emergency exits, are secured and designed to prevent unauthorized access from the outside.

Visitor access to the organisation’s office is prohibited unless authorized and supervised by a host employee. Access to the building where the organization’s dedicated office is located is controlled through a card-based access control system and a manned reception, ensuring that only authorized individuals can enter the premises.

3. Securing Offices, Rooms and Facilities

The office layout is configured in a manner that prevents sensitive information or activities from being visible and audible from the outside, or readily available to any unauthorized person. Depending on the sensitivity of the information handled, restricted access to certain rooms/areas inside the office is implemented.

4. Physical Security Monitoring

The co-working space provider is responsible for physical security monitoring of shared areas. This includes CCTV surveillance and staffed reception.

Within the organization’s dedicated, lockable office unit, physical monitoring is more limited due to its private and self-contained nature. The organization ensures the office is secured when unattended, including locking doors and maintaining a key register, tracking who has access to the office.

In the event of a suspected physical security incident (e.g., unauthorized access, theft, signs of forced entry or tampering), the incident will be reported immediately to the co-working space management for necessary actions.

5. Protecting Against External and Environmental Threats

The organization’s dedicated office is located within a professionally managed co-working facility that provides baseline protection against external and environmental threats. The building is equipped with CCTV and access control systems, fire detection and suppression systems and secure building structure.

Any signs of physical damage, hazards, or security risks shall be reported to the co-working space management for necessary actions.

6. Working in Secure Areas

The organization’s operations involving sensitive information are conducted within a dedicated, secure office unit located inside a co-working facility. This unit is physically separated from shared workspaces and is accessible only to authorized personnel with assigned keys.

Employees are instructed not to leave confidential materials (printed or digital) unattended or visible when not in use and avoid discussing sensitive matters in common or public areas of the co-working space.

7. Clear Desk and Clear Screen

Clear desk rules for papers and removable storage media and clear screen rules for user endpoint devices are enforced in line with the organisation's *Clear Desk and Clear Screen Policy.*

Employees are advised to lock away sensitive information (e.g., on paper or storage media) in a cabinet under lock and key when not required and when their desk is unattended. Employees' endpoint devices should always be locked and configured with an automatic timeout controlled by a user authentication mechanism when unattended after 5 minutes. Employees should not leave written sensitive information such as password on their laptops/desktops. Users shall not tamper with the IT resources, causing performance degradation, service instability or compromising operation efficiency, security and fair use of resources. That can include user dropping of hardware (be it accidentally or intentionally).

When using printers, everyone is advised to collect outputs immediately and stand next to the printer to ensure that only them can collect their printouts. Meeting notes on the boards and other types of display shall be cleared when no longer required (e.g., at the end of the meeting).

8. Equipment Siting and Protection

The work area layout should be designed such that equipment and other information assets cannot be viewed from public areas. Screens that may display sensitive information must be sited away from positions where unauthorised people might view them.

Asset owners shall ensure that the equipment under his/her responsibility is maintained in accordance with the manufacturer's instructions (if any) to ensure it remains in effective working order.

Appropriate environmental conditions such as air conditioning are provided in the offices and its good condition is ensured by the building management.

Equipment with media that is to be re-used must have all of its data and software erased prior to disposal or reformatted for re-assignment to a new asset owner in line with *ISMS-PHY-02 Storage Media Handling.*

9. Security of Assets Off-Premises

Any device used outside the organisation's premises which stores or processes information (e.g., user endpoint devices) shall be authorized through the *ISMS-PPL-01-F3 Company Asset & Access Issuance Form,* and employees shall comply with *ISMS-PPL-04 Guidelines for Remote Working.*

10. Supporting Utilities

The organization's dedicated office unit operates within a co-working facility that provides essential supporting utilities necessary for business continuity, including electrical power, air conditioning and water supply.

The organization coordinates with the co-working space management to monitor the reliability of these utilities and report any issues that could impact operational security or business continuity.

The co-working space provides managed network connectivity, including internet access and internal networking infrastructure. The organization leverages this service while implementing its own security controls, such as VPNs, firewalls, and endpoint protection, to secure data and communications.

11. Cabling

The co-working space provider is responsible for the installation, management, and maintenance of all cabling infrastructure within the building, including network and power cables. Cords and cables are protected by suitable covers and are not routed in walkways which presents a trip hazard that may cause damage.

12. Equipment Maintenance

The organization maintains the reliability and security of its key IT assets, primarily cloud services and laptops.

Maintenance and updates of cloud infrastructure and applications are managed by the cloud service providers, following their established service and security standards. The organization monitors service health, applies necessary configuration updates, and ensures timely patching of cloud-based resources.

Laptops issued to employees undergo regular maintenance, including operating system updates, security patches, and antivirus scans. Only authorized IT personnel perform maintenance and troubleshooting. Users are responsible for reporting any faults or issues promptly to IT personnel.

13. Secure Disposal or Re-use of Equipment

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use. For more details on secure disposal of storage media, refer to *ISMS-PHY-02 Storage Media Handling.*

The organization is responsible for removing all its assets from the premises upon relocation or at the end of a lease term if not renewed.

Prior to disposal, resale, or donation, all labels, markings, or identifiers that associate the assets with the organization must be completely removed to protect sensitive information and organizational identity.