Physical and Environmental Security Procedure

Version 1 - Approved by Rishabh

Contents

1. Objective

An Information Security Management System (ISMS) has been implemented at Superhawk AI to protect the organization's sensitive information from unauthorized access, loss, or inaccuracy.

Through this document, Superhawk AI has recognized the need and established guidelines to incorporate physical and environmental security to prevent unauthorized access to physical spaces, avoid damage to assets, and prevent interference with the company’s information and information processing facilities.

2. Scope

The scope of the Physical and Environmental Security procedure covers Superhawk AI’s cloud-hosted production environments and supporting functions, employee devices (laptops/workstations) that access company systems, and physical assets owned or issued by Superhawk AI. Physical office premises where no production servers or customer data are hosted are out of scope for production facility controls but remain in scope for staff device and asset protection.

3. Process Responsibilities

3.1 Information Security Officer

Reviewing the device security status checks.

3.2 Engineering Department and HR

- Allocation and deallocation of systems/devices.
- Training of users regarding the use of physical assets like Laptops.
- Ensuring that the return of information assets and removal of access to systems is done appropriately.

4. Physical Security Requirements

- Superhawk AI is a software-as-a-service company; production infrastructure and customer data are hosted on third-party cloud providers (AWS and GCP). Physical security of those cloud datacenters is managed by the respective cloud providers.
- The Information Security Officer, with support from Legal and Engineering, shall review cloud provider agreements and obtain relevant security documentation (e.g., provider ISO certificates, SOC 2 reports) at least annually to verify controls for confidentiality, integrity, and availability of Superhawk AI data.
- Because infrastructure is cloud-hosted, on-premise office premises are out of scope for production datacenter controls; however, physical security expectations for employee devices and office access (badge control, visitor handling) apply as part of asset protection.

5. Requirement for Physical Assets

- Each user is responsible for protecting company assets issued to them, including laptops and portable devices, following the Asset Management Policy.
- HR shall ensure employees, contractors, and temporary staff with access to company assets receive information security onboarding that covers protection of unattended equipment, secure handling of PII and business data, and procedures for returning assets on exit.
- All staff must not leave equipment unattended in public areas and must secure devices with company-approved protections (full-disk encryption, strong passwords, screen lock). Active sessions should be terminated or locked when not in use. These practices will be reinforced through periodic training and referenced in the Device Security and Acceptable Use policies.

6. Clear Desk & Clear Screen Policy

Clear Desk Policy applies to paper (hardcopy) and laptops to ensure unauthorized personnel do not have access to Superhawk AI information. While it is strongly recommended not to use paper assets – in cases where it is required, the following will be applicable:

6.1 Clear Desk Policy

- Client Confidential / Superhawk AI Confidential paper assets shall be stored securely (locked cabinets) when not in use and must not be left unattended in shared or public areas.
- Passwords must always be memorized and must never be written down on paper.
- All workspaces must always be left clear before leaving for longer periods of time.
- In case of an incident associated with information loss, the matter must be immediately escalated to the Information Security Officer and should follow the Incident Management Procedure.

6.2 Clear Screen Policy

- Users shall lock their computers when leaving their desks and log off when leaving for an extended period of time. This ensures that the contents of the computer screen are protected from prying eyes, and the computer is protected from unauthorized access.
- Use of Laptop / Desktop Privacy Screens shall be considered in case required.
- Users shall not keep files/shortcuts on the desktop screen; and
- Users shall delete all the files from the recycle bin on a regular basis.

7. Document Security Classification

Company Internal. Please refer to the Data Classification Policy for more details.

8. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

9. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

10. Schedule

This document is to be reviewed annually and whenever significant changes occur in the organization, including changes to cloud providers (AWS, GCP), changes in workforce composition (e.g., introduction of contractors), or after any material security incident.

End of Physical & Environmental Security Procedure. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026