Asset Management Procedure

Version 1 - Approved by Rishabh

Contents

1. Objective

The objective of this document is to describe a formal procedure to be followed for maintaining, handling, and protecting all the information assets of Superhawk AI.

2. Scope

This procedure applies to all employees, contractors, and temporary staff at Superhawk AI who use or have access to Superhawk AI's information assets and data, including assets hosted on cloud platforms (AWS, GCP), code stored in GitHub, and data accessible via Google Workspace.

3. Asset Management Procedure

3.1 Inventory of Assets

- At all times, the updated inventory of assets shall be maintained.
- Inventory of infrastructure, code repositories, and cloud resources is maintained using native cloud provider inventories (AWS/GCP) and GitHub repository listings. Google Workspace is used to track email accounts and related user identities. A list of information assets like infrastructure, code repositories, software, and people assets are automatically maintained using cloud service providers, version control systems, identity providers, or HRMS applications (if applicable), respectively.
- For assets where inventory cannot be maintained automatically, it is the responsibility of the Information Security Officer to document the use of other software assets that have access to sensitive information.
- Superhawk AI allows employees to bring their own laptops or Superhawk AI issued laptops in some cases. For all such end-point devices, employees are responsible for reporting the device that they use to access Superhawk AI's data. The guidelines to maintain the security of endpoint devices shall be made available to all users through the Endpoint Security Policy.
- It is the responsibility of the People Operations Head and People Operations team to ensure that all employees have reported the status of devices used by them.
- The inventory of assets should also include the asset owner. Asset owners shall be responsible for maintaining and updating the inventory of the assets.
- The Information Security Officer must verify the information asset inventory once it is created and at least on an annual basis thereafter.

3.2 Managing Infrastructure Assets

- Any new infrastructure asset acquired by Superhawk AI should automatically be tracked in the inventory that is maintained. In case it is not tracked automatically or in the event of a non-success, the Infra Operations Person or Information Security Officer must ensure the asset list is updated periodically.
- The Infra Operations Person is responsible for the classification of all infrastructure assets hosted on AWS and GCP. Classification is based on the type of data the assets process (including PII, business/operational data, and behavioral data) and their criticality to services, consistent with the Data Classification Policy. The classification scheme is based on the type

of data that the assets process and their criticality to services. The classification should be based on the Data Classification Policy.
- Based upon the classification of assets, there are security controls implemented to safeguard the integrity of the asset. These security controls are tracked along with the inventory of assets.
- Monitoring of infrastructure security controls leverages cloud provider services (e.g., AWS Config, GCP Security Command Center) and integrations with GitHub where available; automated alerts are configured to notify responsible owners. The status of the security controls is automatically monitored through tools that integrate with cloud service providers/version control systems.
- If any of the security controls fail, an automatic alert is sent to the Infra Operations Person, who will be responsible for implementing the necessary changes promptly.
- If the controls are not implemented within the stipulated time, the security gaps are escalated automatically to the Information Security Officer, who will need to take necessary rectifying measures.

3.3 Managing End Point Assets

- Superhawk AI allows employees to “Bring your own device” for their company operations. The list of all the end-point devices is maintained.
- All employees need to report the devices that they use to access Superhawk AI’s data.
- If maintained manually, it is the responsibility of the Information Security Officer to ensure that periodic requests are sent at least once a quarter to all employees to report their device security status.
- It is the responsibility of users to follow the recommended steps below to ensure the security of endpoints:
    - Superhawk AI staff and contractors are responsible for installing critical firmware and software updates on the endpoints they use or where they’re the assigned owner.
    - All endpoints with access to critical data are required to run up-to-date antivirus/endpoint protection software; where company-issued devices are provided, Superhawk AI will provision and manage endpoint protection.
    - All endpoints with access to critical data must enable disk encryption (e.g., FileVault on macOS or BitLocker on Windows); for company-issued devices, encryption will be enforced by device management.
    - As detailed in the access control policy, Superhawk AI staff members should use strong passwords to protect against unauthorized access to their system or any services they use. While it is not mandatory, it is recommended to use a password manager.
    - All endpoints with access to critical data must enable automatic screen-lock with a reasonable inactivity period; company-issued devices will have this configured via device management where applicable. While the screen lock will protect the device in most cases, it is recommended not to leave the computer unattended and unlocked.
    - Employees must immediately report lost, stolen, or damaged devices to the Superhawk AI management, which will then attempt to constrain access to production systems and customer data through the exposed device.
    - Employees must follow the removable media guidelines outlined in the Asset Management and Physical and Environmental Security policies.

- Endpoints may be verified for compliance with this policy through various methods, including, but not limited to, periodic reviews, automated monitoring, and internal and external audits.

3.4 Review of Assets

The Infra Operations Person and the Information Security Officer must review the list of Infrastructure assets, cloud resources (AWS/GCP), and critical systems at least annually; reviews should also occur when major changes to cloud architecture, GitHub repository structure, or third-party integrations (including Google Workspace changes) occur.

4. Document Security Classification

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

5. 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.

6. 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.

7. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization or its cloud infrastructure, code repositories (GitHub), or third-party services (e.g., Google Workspace).

End of Asset Management 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