Asset Management Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

The objective of this document is to provide a framework to ensure that Superhawk AI's information assets and data are protected and handled appropriately.

2. Scope

This policy applies to all information assets, systems, and services used in the delivery, development, and support of Superhawk AI's SaaS products and internal operations. It covers cloud-hosted resources on AWS and GCP, code and related artifacts stored in GitHub, data stored in Google Workspace, and employee devices (laptops and workstations) that access corporate resources. The policy applies to all employees, contractors, and third-party service providers who process, store, or access Superhawk AI data.

3. Policy Statement

The Asset Management Policy is established to ensure that all Superhawk AI assets are classified and appropriately protected and that information handling or exchange of information is in accordance with this classification. This shall prevent unauthorized disclosure, modification, removal, or destruction of assets and interruption to business activities.

4. Asset Management

4.1 Types of Assets

The following are examples of the types of assets that need to be considered as Information Assets:

- Infrastructure Assets: databases and data files, servers, and version control systems.
- Software Assets: application software, system software, development tools, and utility software.
- Physical Assets: computer equipment, communications equipment, removable media, and other equipment.
- Service Assets: computing and communications services, general utilities such as heating, lighting, power, air-conditioning, and third-party suppliers.
- People Assets: employees (full-time and part-time), customers, contractors.
- Paper Assets/E-Documentation: contracts, agreements, non-disclosure agreements, system documentation, user manuals, training material, operational or support procedures, business continuity plans, fallback procedures, audit trails, and archived information.

4.2 Responsibility of Assets

- All information and associated assets shall have an individual or department with management responsibility assigned to control the production, development, maintenance, use, and security of the information asset.

- Each asset shall have an Asset Owner; for technical assets the Asset Owner is typically a named engineering manager or product owner, and for cloud resources the cloud infrastructure owner (e.g., the team responsible for AWS or GCP resources) shall be identified. Where operational custody differs from ownership, a Custodian (for example, an IT administrator or contractor) may be nominated.
- The owner shall be responsible for the following:
    - Ensuring that information and assets associated with information processing facilities are appropriately classified.
    - Defining and maintaining the security of the assets along with helping the Information Security Officer periodically review access restrictions and classifications, taking into account applicable access control policies.
- As information is important and pervasive throughout Superhawk AI, all users have an important role and a responsibility to protect the information entrusted to them. All users who may come into contact with sensitive information (non-public) are expected to familiarize themselves with the Asset Management Policy and the Asset Management Procedure.

4.3 Inventory of Assets

- At all times, the updated inventory of assets shall be maintained.
- Asset inventories shall include cloud resources (AWS and GCP projects/accounts), GitHub repositories, Google Workspace resources, employee device records, and third-party SaaS subscriptions. Inventories shall record asset ID, asset classification, owner, location, and lifecycle status.
- There should be owners assigned to maintaining the asset inventory. The owners may be different based on the type of asset.
- At the minimum, the inventory of assets needs to include an asset ID, an asset classification, and an asset owner.

4.4 Acceptable Use of Assets

- Acceptable use of assets associated with information assets shall be clearly defined.
- All users (employees, contractors, and third-party personnel) who use or interface with assets associated with Superhawk AI shall acknowledge their awareness of acceptable use through required onboarding training and periodic refresher training. Use of corporate Google Workspace accounts and GitHub access must follow account management and least-privilege principles.

4.5 Return of Assets

Upon termination or contract end, employees and contract partners shall return or securely transfer all physical information assets. For cloud accounts and access, IT or Cloud Operations shall disable or remove access and ensure transfer or archival of any owned resources. Device return procedures shall be followed for company-owned laptops; if devices are personal but used for corporate access, corporate data shall be wiped or access revoked according to the Offboarding Procedure.

5. Data Classification

- Information assets shall be classified based on their business value, legal requirements, sensitivity, and criticality to the organization.
- Classification labels used at Superhawk AI include Public, Internal, Confidential, and Restricted. Personal Identifiable Information (PII) and data subject to GDPR shall be treated at minimum as Confidential or Restricted depending on sensitivity and legal requirements.
- It is important to understand the type of data the information asset processes to ensure that assets are handled appropriately. Please refer to the Data Classification Policy for more details.

6. Management of Removable Media

Use of removable media (USB drives, external HDD/SSD) for transfer or storage of corporate data is prohibited except where approved by Information Security for specific business needs. Approved use requires encryption, asset owner approval, and logging of the device in the asset inventory. Unauthorized use of removable media is non-compliant.

7. Disposal of Media

- Disposal of media, both electronic and physical, is important to ensure that data is protected from exposure to unauthorized people.
- Electronic backups and primary data stored within managed cloud services (AWS, GCP, Google Workspace) rely on vendor-provided disposal controls; disposal of such media is handled in accordance with vendor documentation and contractual obligations. For company-owned physical media and devices, disposal shall follow secure wipe or physical destruction procedures consistent with data classification; device disposal must be coordinated with IT and Asset Owners.
- Media shall be disposed of securely, following the formal guidelines when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the Data Classification policy.
- Please refer to the Media Disposal policy for guidelines and details.

8. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

9. 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.

10. Responsibilities

The Information Security Officer (or Security Lead) is responsible for approving and reviewing policy and related procedures. Cloud Engineering, IT, and Engineering Managers shall be

responsible for implementing the relevant sections of the policy in their area of operation.

11. Schedule

This document shall be reviewed at least annually and additionally whenever significant changes occur in infrastructure, third-party providers (e.g., AWS, GCP, GitHub, Google Workspace), services, or applicable legal/regulatory requirements (such as GDPR).

End of Asset Management Policy. 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