Information Security Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

While providing Superhawk AI’s service to clients, Superhawk AI’s staff members and vendors acquire access to the client's privileged and sensitive information. Each of Superhawk AI's clients places an enormous amount of trust that their data is created, stored, shared, and transmitted securely.

The loss of any client data or services due to unauthorized access, intrusion, theft, natural or cyber disasters, or cyber-attacks diminishes the client's trust as well as significantly damages Superhawk AI’s reputation as an advocate for companies to develop, implement and maintain systems to prevent the loss of intellectual property and other confidential information.

The purpose of this policy document is to define the direction, principles, and basic rules for information security management within Superhawk AI. This document describes the management's vision and commitment to effectively protect "confidentiality," maintain "integrity," and ensure the "availability" of its information assets and to respond and recover from information security incidents when they arise.

Information security is deemed to safeguard three main objectives:

- Confidentiality – Data and information assets must be confined to people authorized to access them and not be disclosed to others.
- Integrity – Keeping the data intact, complete, and accurate, and information systems operational.
- Availability – An objective indicating that information or system is at the disposal of authorized users when needed.

2. Scope

This policy applies to all employees, contractors, and third-party vendors of Superhawk AI who access, process, store, or transmit organizational or client data, including Personal Identifiable Information (PII), business and operational data, and behavioral data. It covers information assets and activities hosted in cloud platforms used by Superhawk AI (including AWS and GCP), data stored on employee devices (laptops/workstations), code repositories in GitHub, and services tied to Google Workspace email. The scope includes all digital systems, applications, services, and related processes used to develop, operate, and support Superhawk AI's SaaS offering, as well as any physical media or documentation that contain organizational or client information.

3. Policy Statement

- Superhawk AI shall establish, implement, and maintain a holistic and robust Information Security Management System (ISMS). ISMS is defined as the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

- The ISMS shall have adequate and appropriate arrangements which shall enable it to effectively protect "confidentiality," maintain "integrity" and ensure "availability" of its information assets and to respond and recover from information security incidents when they arise.
- While planning the ISMS, Superhawk AI shall consider its internal and external issues along with the requirements of the interested parties and determine risks and opportunities that could affect the activities supporting the provision of its products and services. The top management shall provide the required resources and sufficiently contribute towards the ISMS, ensuring it achieves its intended outcome(s).

4. Information Security Requirements

Information and supporting technology — including cloud-hosted infrastructure on AWS and GCP, code repositories in GitHub, collaboration and email via Google Workspace, and employee devices — are critical business assets. Confidentiality, integrity, and availability of these assets are essential to legal compliance (including SOC 2 and GDPR), customer trust, and business continuity. Security controls shall combine technical measures (for example, cloud provider IAM, encryption, network security configurations, and endpoint protection on employee devices) with administrative controls (policies, training, vendor management) and physical protections where applicable. Third-party SaaS and cloud providers' security responsibilities and assurances (e.g., AWS and GCP shared responsibility models, Google Workspace controls) shall be documented and validated as part of vendor management.

5. Information Security Objectives

The objectives of the Information Security Policy are:

- To establish and maintain an ISMS aligned with Superhawk AI’s SaaS business strategy and applicable frameworks (SOC 2, ISO 27001, GDPR).
- To protect and safeguard customer and organizational information, including PII, business data, and behavioral data, stored or processed in AWS, GCP, Google Workspace, and on employee devices.
- To reduce risk arising from software development, cloud operations, and third-party services through secure development practices, vendor due diligence, and configuration management.
- To ensure that information assets and code repositories (GitHub) are inventoried and assigned appropriate protection levels.
- To ensure that information and information systems are available only to authorized users through role-based access controls and least privilege.
- To provide customers with means to exercise PII rights (access, correction, erasure) in accordance with contractual obligations and GDPR requirements.
- To ensure PII processed under contract is only processed per customer instructions and not for any independent purpose.
- To achieve and maintain compliance with applicable regulatory requirements related to data collection, storage, processing, transmission, and disclosure.
- To allocate resources to establish, implement, operate, monitor, review, and improve information security controls.

- To maintain an awareness program ensuring employees, contractors, and relevant vendors understand and fulfill their information security responsibilities.
- To produce and maintain supporting procedures and guidelines (e.g., access control, incident response, asset management) and ensure compliance with them.
- To periodically review and update information security objectives and controls in response to business changes, incidents, or audit findings.

6. Segregation of Duties

- Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization’s assets.
- While assigning responsibilities, conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.
- Care shall be taken that every individual may access, modify, or use assets with proper authorization or detection. The possibility of collusion should be considered while designing the controls.

7. Contact with Special Interest Groups

Based on requirements and validated procurement, Superhawk AI may engage independent security consultants or managed security service providers for specialized advice, penetration testing, or architecture reviews. Participation in relevant industry forums and information sharing groups (for example, cloud provider security communities or SaaS security groups) may be used to stay current on threats and best practices.

8. Contact with Authorities

Where required, Superhawk AI shall maintain documented points of contact with law enforcement, regulatory authorities relevant to data protection (including GDPR supervisory authorities where applicable), emergency services, and telecommunications providers. Contact details and escalation procedures shall be maintained within the incident response plan to ensure timely engagement during security incidents or data breaches.

9. Information Security in Project Management

Information security requirements shall be integrated into project and product management practices. For software development projects, this includes threat modeling, secure coding guidance, code review in GitHub, dependency management, and security testing prior to deployment. Cloud configuration reviews and change control shall be performed for AWS and GCP resources. Project owners must document security requirements and obtain approval from the Information Security Officer or delegated security reviewer before production deployment.

10. Reporting of Security Incidents

All staff, contractors, and third-party vendors must report suspected or confirmed security incidents immediately to the Information Security Officer and via Superhawk AI's incident reporting channel

(for example, the internal incident reporting workflow or designated email/Slack channel). The incident response plan defines notification timelines, roles, and escalation paths, including obligations for breach notification under GDPR and contractual requirements.

11. Maintenance of Policy

- Compliance with this policy and supporting policies shall be audited yearly. Exceptions identified during the audit shall be immediately and appropriately addressed.
- The security policy shall be reviewed annually, except in the event of a major change in the organization or the environment affecting the organization, in which case it shall be reviewed on a need basis.
- The security policy shall be reviewed and revised whenever a major security risk or incident is identified.

12. Supporting Policies

The following policy documents shall support the information systems security policy at a minimum:

12.1 Human Resources Security Policy

The purpose of this policy is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

12.2 Risk Assessment & Management Procedure

The purpose of this procedure is to ensure that guidelines related to understanding and managing risks that may affect information security are provided.

12.3 Access Control Policy

The purpose of this policy is:

- To limit access to information and information processing facilities.
- To ensure authorized user access and to prevent unauthorized access to systems and services.
- To make users accountable for safeguarding their authentication information.
- To prevent unauthorized access to systems and applications.
- Segregation of duties.

12.4 Asset Management Policy

The purpose of this policy is:

- To identify Superhawk AI’s assets and define appropriate protection responsibilities.
- To ensure that information receives an appropriate level of protection in accordance with its importance to Superhawk AI.
- To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

12.5 Operations Security Policy

The purpose of this policy is to ensure the protection of information through daily operations that take place in providing Superhawk AI's services.

12.6 Acceptable Usage Policy

- To ensure that all employees at Superhawk AI are aware of the acceptable use of assets and formal cybersecurity guidelines to ensure best security practices.
- To ensure that Superhawk AI's information is protected when accessed, processed, or stored at teleworking sites.

12.7 Compliance Policy

The purpose of this document is to ensure Superhawk AI complies with all legal and regulatory requirements to ensure the proper functioning of all business domains.

12.8 System Acquisition and Development Policy

The purpose of this policy is to ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems that provide services over public networks.

12.9 Physical and Environmental Policy

This policy helps to prevent unauthorized physical access, damage, and interference to Superhawk AI's information and information processing facilities.

12.10 Business Continuity Management Policy

The purpose of this policy is to ensure that business continuity is embedded in Superhawk AI's scope of operations.

12.11 Vendor Management Policy

The purpose of this policy is to ensure the protection of Superhawk AI's assets that are provided by third-party suppliers.

12.12 Incident Management Policy

This policy helps the management of any information security incidents that may compromise confidentiality, integrity, or availability of data and services by Superhawk AI.

13. Document Security Classification

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

14. 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.

15. Responsibilities

- The Information Security Officer (or designated Security Lead) has the ultimate authority over the Information Security Policy and approves and authorizes all changes to the Information Security Policy.
- The Information Security Officer has executive authority over information security and works with Executive Management to approve, authorize, and issue all documentation.
- The Information Security Officer is responsible for the development and maintenance of all ISMS documentation.
- The Information Security Officer shall schedule periodic internal audits with the help of either internal teams or external consultants.
- The Information Security Officer, along with the Head of Engineering, is responsible for building and maintaining privacy and security programs that define, develop, maintain, and implement policies and processes to protect PII across cloud services (AWS, GCP), Google Workspace, GitHub, and employee devices.

16. Schedule

This document is to be reviewed annually and whenever significant changes occur in the organization, such as major changes to cloud infrastructure (AWS/GCP), adoption of new third-party services (e.g., GitHub integrations or Google Workspace changes), or changes in applicable regulatory requirements (SOC 2, ISO 27001, GDPR).

End of Information Security 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