Compliance Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

The purpose of this policy is to establish guidelines for the management of regulatory and legal compliance requirements for systems in accordance with applicable standards such as ISO 27001:2013, ISO 27001:2022, SSAE 18(SOC 2), and other standards.

2. Scope

This document applies to all Superhawk AI processes, services, and operations that are in scope of the Information Security Management System (ISMS). In practice this includes SaaS product development and delivery activities hosted on cloud platforms (AWS and GCP), code and related artifacts stored in GitHub, business email and related user accounts managed via Google Workspace, and employee devices (laptops/workstations) used to access company systems and customer data. The scope covers processing of Personal Identifiable Information (PII), business and operational data, and behavioral data collected or processed by the organization.

3. Policy Statement

The information security management system of Superhawk AI shall be established and operated with due consideration for compliance with statutory, regulatory, or contractual obligations as well as any specific security requirements.

4. Compliance Policy

4.1 Identification of Applicable Legislations & Compliance Requirements

Superhawk AI shall maintain a documented register of applicable legal, regulatory, and contractual compliance requirements relevant to its SaaS operations, including but not limited to SOC 2, ISO 27001, and GDPR obligations. The register shall identify requirement source, applicability, responsible owner, and review frequency. The register will be reviewed at least annually or when there are changes in services, laws, or contractual obligations.

4.2 Intellectual Property Rights

Superhawk AI shall comply with license terms for third-party software and protect client intellectual property processed or stored within its SaaS platform. Use of open-source components in GitHub repositories shall follow the organization's approved licensing and dependency review processes.

4.2.1 Protection of Organizational Records

Records related to information security, compliance evidence, audit logs, and configuration baselines shall be retained and protected in accordance with statutory, contractual, and business requirements. Where storage is provided by cloud vendors (AWS, GCP) or Google Workspace, Superhawk AI relies on vendor controls for infrastructure availability and physical protection while ensuring access controls, backups, and retention settings are configured per organization policy.

4.2.2 Data Protection and Privacy of Personal Information

Superhawk AI shall process personal data in accordance with applicable data protection laws including GDPR. Data subject rights, lawful basis for processing, data minimization, and data retention requirements shall be documented and implemented. Cloud storage, processing, and backups of PII shall use encryption and access controls provided by AWS and GCP; Google Workspace shall be configured to enforce appropriate controls for email and account data.

4.2.3 Prevention of Misuse of Information Processing Facilities

Use of information processing facilities (including GitHub, cloud consoles, and Google Workspace) must comply with the Acceptable Usage policy and Code of Business Conduct. Violations will be addressed through disciplinary processes applicable to employees and contractors.

4.2.4 Compliance with Security Policies, Standards, and Technical Compliance

Department heads and team leads are responsible for ensuring security procedures are implemented within their areas, including secure development practices in GitHub, appropriate IAM controls in AWS and GCP, and secure configuration of Google Workspace. Where responsibilities are shared with cloud vendors, teams shall ensure vendor configurations meet organizational requirements.

4.2.5 Information Systems Audit Considerations

Superhawk AI shall engage competent internal or external auditors to perform periodic audits of information security and compliance controls. Audit activities will be scheduled to minimize operational disruption. Audit tool access and audit data (logs, reports) shall be protected and access limited to authorized personnel. Findings will be tracked, remediated, and verified by the Information Security Officer or designated owner.

- Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed upon to minimize the risk of disruptions to business processes.
- Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

5. Document Security Classification

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

6. 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 violate 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.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. The Information Security Officer shall maintain the compliance register, coordinate audits, and act as the point of contact for regulatory and contractual compliance matters. Team leads and department heads are responsible for implementing controls within their areas, including secure configuration of AWS, GCP, GitHub, and Google Workspace. Employees and contractors must follow applicable policies and report compliance concerns to the Information Security Officer.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur within the organization, such as onboarding new cloud platforms, major changes to the SaaS product, changes in applicable laws (e.g., GDPR), or significant changes to third-party vendor relationships.

End of Compliance 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