Vendor Management Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

Superhawk AI depends on third-party vendors for a range of services. Some of these services are critical for Superhawk AI to meet its security commitments and provide uninterrupted services to its customers. This policy provides the guidelines for managing vendor relationships that affect the services we provide with an aim to minimize the risk associated with using third parties.

2. Scope

This policy applies to all third-party vendors and service providers engaged by Superhawk AI that are critical to the delivery, operation, or security of Superhawk AI's SaaS platform or that process, store, or transmit Personal Identifiable Information (PII), Business & Operational Data, or Behavioral Data. It includes cloud infrastructure providers (e.g., AWS, GCP), code and development platform providers (e.g., GitHub), email and collaboration providers (e.g., Google Workspace), and any other vendors with access to employee devices, customer data, or production environments.

3. Policy Statement

Superhawk AI is committed to exercising caution when sharing critical data with third-party vendors. It is essential to recognize that each instance of data shared with a vendor expands the potential attack surface of that data. Given our reliance on multiple third-party services, there is a need to share specific data. This policy establishes a deliberate process for evaluating critical third-party vendors, ensuring we maintain the highest data security and risk assessment standards.

4. Vendor Management

4.1 Information Security in Vendor Relationships

- Information security requirements for mitigating the risks associated with the vendor’s access to Superhawk AI’s assets shall be agreed upon with the supplier and documented in the form of agreements or contracts.
- Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party shall be defined within these agreements or contracts.
- For third-party personnel who have access to Superhawk AI’s assets, it is essential that they acknowledge the latest version of Superhawk AI’s information security policies.
- Security controls and service levels specified in the contracts or agreements shall be implemented, operated, and maintained by the vendor.
- Contracts/Agreements shall include information security requirements to ensure compliance with Superhawk AI’s security policies and procedures.
- Non-Disclosure / Confidentiality agreements to protect Superhawk AI’s information assets shall be signed by vendors, third parties, contractors, and subcontractors of the vendors, as applicable.

4.2 Vendor Risk Assessments and Service Delivery Reviews

- Superhawk AI shall maintain an inventory of all vendors that are critical to the SaaS platform or that handle PII, Business & Operational Data, or Behavioral Data. This inventory will record vendor name, service provided, data types accessed, contract owner, and contact information.

- A vendor risk assessment shall be performed prior to onboarding any vendor identified as critical or handling sensitive data. Assessments shall evaluate security posture, compliance certifications (e.g., SOC 2, ISO 27001), data handling practices, access requirements, and subcontractor usage.
- For vendors that host or process customer or sensitive data (e.g., AWS, GCP, GitHub, Google Workspace), evidence of appropriate controls or certifications shall be collected and retained as part of the assessment.
- Higher-risk vendors shall undergo periodic reassessment at least annually or when there are significant changes to the service, scope of data processed, or incident reports. Lower-risk vendors shall be reviewed on a biennial basis or as determined by the Information Security Officer.

4.3 Review Vendors and Managing Changes to Vendor Services

- The vendor inventory and associated risk assessments shall be reviewed at least annually and updated whenever a vendor’s scope of access, data processed, or criticality changes.

- Business function managers must notify the Information Security Officer and the contract owner before engaging a new vendor or materially changing an existing vendor’s level of access or services.
- Changes to vendor services that affect data residency, encryption, backup arrangements, or access controls shall trigger a re-assessment and, where necessary, contract amendments to address security and compliance requirements.

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 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.

7. 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. Specific responsibilities include maintaining the vendor inventory, coordinating vendor risk assessments, retaining evidence of vendor compliance (e.g., SOC 2 or ISO 27001 reports), and coordinating remediation or contract

updates for identified vendor risks. Business function managers are responsible for initiating vendor assessments and notifying the Information Security Officer of vendor changes.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization, including changes to the vendor environment, introduction of new cloud providers (e.g., AWS, GCP), or changes in applicable regulatory requirements (e.g., GDPR). Vendor risk assessments shall follow the review cadence specified in section 4.2.

End of Vendor 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