Vendor Management Procedure

Version 1 - Approved by Rishabh

Contents

1. Objective

The objective of this document is to outline the responsibilities and process to be followed while managing relationships with third parties or vendors critical to Superhawk AI's services.

2. Scope

This document applies to all staff, contractors, and contractors' personnel at Superhawk AI who engage, provision, or use third-party vendors whose services are critical to the operational integrity, availability, or security of Superhawk AI's SaaS products and platforms, or with whom customer PII, business/operational data, or behavioral data is shared.

3. Vendor Management Procedure

3.1 Responsibilities

- It is the responsibility of the Information Security Officer, in coordination with Business Heads and the Procurement function, to ensure the following:
    - Identifying all Superhawk AI vendors and suppliers.
    - Vetting the security controls of third parties before establishing a third-party contract relationship.
    - Ensuring an approved and up-to-date Superhawk AI vendor/supplier agreement is in place and has been signed by every third party.
    - Maintaining a current and accurate listing of all Superhawk AI vendors and suppliers.
    - Monitoring third parties for adherence to provisions within vendor/supplier agreements (where applicable), service level agreements (SLAs), and contractual security requirements, as applicable.
    - Performing periodic or continuous reviews of security measures implemented by third-party service providers.
- Business heads and team leads must notify the Information Security Officer whenever they are contracting a new vendor or in case of any changes to services provided by existing vendors.

3.2 Managing Contracts and Service Level Agreements

- Once a vendor has been selected, it is the responsibility of the Business Heads and Information Security officer to ensure that an official contract has been signed between Superhawk AI and the vendor.
- In the case of using SaaS vendors, subscription-based products may be chosen to carry out business functions, and in such cases, signing contracts is not possible. For all such cases, the Information Security Officer must review the vendor's published terms of service and privacy policy, and ensure contractual or documented evidence of acceptable data handling and security controls where possible (for example, through a signed Data Processing Agreement when the vendor processes customer data).
- The Information Security Officer must ensure that Non-Disclosure Agreements or Confidentiality agreements are in place with vendors who have access to sensitive data. For

cloud infrastructure providers and major SaaS services used by Superhawk AI (for example, AWS, GCP, GitHub, and Google Workspace), the organization will rely on vendor-managed controls supplemented by contractual terms such as Data Processing Agreements and vendor security documentation. In case this is not possible, the Information Security Officer must review the privacy policy published by such vendors.

3.3 Vendor Risk Management

- The list of vendors must be identified and maintained by the Information Security Officer in the vendor inventory. This inventory must be reviewed at least once a year by the Information Security Officer and whenever a new vendor is onboarded or an existing vendor's service scope changes.
- Each vendor is evaluated based on the following principles:
    - Impact to Superhawk AI's operations due to unavailability/ breach of vendor services.
    - Vendor's access to Superhawk AI's sensitive data/ information assets.
- Further, Vendors must be assessed for their suitability based on the following considerations:
    - Do we have a way to contact the vendor when we face any service interruptions or degradation?
    - Does the vendor have any information security certifications like SOC2, ISO27001, etc?
    - Is there sufficient information from the vendor to indicate the security practices they follow?
    - In the absence of the above, does the vendor need to be sent a vendor assessment questionnaire?
    - What are Superhawk AI's options if the vendor experiences downtime? What happens if the vendor ceases operations suddenly? Are there other potential vendors that Superhawk AI could work with in such cases?
- Based on the evaluation, the criticality of the vendor services is given below:
    - High
        - Critical services are disrupted
        - The vendor has access to most or all critical data
    - Medium
        - Critical services are functional
        - The vendor has restricted access to critical data
    - Low
        - Minimal impact on critical services
        - Minimal access is provided to the vendor
- Depending upon the business needs and the severity of the risk of data involved, the vendor's certificates or security reports must be collected from the vendor. The Information Security Officer should ensure the validity of these reports.
- For all vendors that carry the highest risk, appropriate due diligence in the form of reviewing their Information security certifications or evaluations through questionnaires is mandatory.

3.4 Vendor Monitoring & Reviews

- The Information Security Officer must review the list of vendors and their criticality at least annually.

- It is the responsibility of the business heads to ensure that they monitor the service being delivered by the vendors. In case of any deficiencies noted, they must inform the Information Security Officer immediately to ensure corrective measures are taken.

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 this procedure and related policies. Business Heads, Procurement, and IT/Platform teams are responsible for implementing vendor onboarding, contract management, and operational monitoring. All staff and contractors must follow vendor engagement controls before procuring or using third-party services.

7. Schedule

This document shall be reviewed annually or when significant organizational changes occur, including changes to cloud infrastructure providers (e.g., AWS, GCP), major SaaS vendor usage (e.g., Github, Google Workspace), or applicable regulatory requirements (SOC 2, ISO 27001, GDPR).

End of Vendor 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