



# Risk Assessment & Management Policy

Version 1 - Approved by Rishabh



# Contents

1. [Objective](#)
2. [Scope](#)
3. [Policy Statement](#)
4. [Risk sources](#)
5. [Risk related concepts](#)
6. [Risk Assessment Policy](#)
7. [Risk Mitigation](#)
8. [Document Security Classification](#)
9. [Non-Compliance](#)
10. [Responsibilities](#)
11. [Schedule](#)
12. [Version history](#)



## 1. Objective

Systematic risk assessments are important because they identify, prioritize, and help track the treatment of risks to Superhawk AI's commitments to its customers and other stakeholders. The purpose of this policy is to have a formalized risk assessment approach for risk identification, analysis, and treatment.

## 2. Scope

This document is applicable to all employees, contractors, and subsidiaries of Superhawk AI that participate in the development, operation, support, or management of the company's SaaS product and related business services within the scope of the ISMS. It covers systems and data hosted on cloud platforms (AWS and GCP), code repositories in GitHub, email and collaboration in Google Workspace, and employee devices used to access corporate resources.

## 3. Policy Statement

Superhawk AI periodically performs an operational risk assessment to identify risks impacting its commitments. Results from the assessment are compiled into a report reviewed by management. Identified security risks are risk-rated, assigned to a risk owner, and tracked to risk treatment completion or acceptance.

## 4. Risk Sources

Some common sources of risk are:

- Risks related to cloud infrastructure and configuration on AWS and GCP (misconfigurations, credential compromise, service outages).
- Risks arising from code repositories and development workflows in GitHub (insecure code, insufficient branching/PR controls, leaked secrets).
- Risks to data processed or stored by the SaaS platform, including PII, business/operational data, and behavioral data.
- Risks from employee and contractor devices (lost/stolen laptops, unpatched workstations) that access corporate systems.
- Risks related to email and collaboration tools (Google Workspace) such as phishing, accidental data exposure, and unauthorized sharing.
- Possibility of fraud affecting our ability to achieve our business objectives.
- Changes to the regulatory, economic, and physical environment in which the entity operates, including GDPR and other applicable regulations.
- Risks associated with third-party vendors and managed services.

Please refer to the Vendor Management Policy for guidelines on assessing vendors.

## 5. Risk related concepts

### 5.1 Threats

A Threat is a possible situation or activity which may be deliberate, accidental, or caused by nature resulting in the degradation of the operational status of the organization. This may include but is not limited to service outages, data theft, physical harm, or financial loss.



## 5.2 Impact

Impact measures the extent of damage in the outcome of a threat event (usually loss or disadvantage). It represents the magnitude of harm expected from a fully materialized threat. Typical outcome scenarios for which the impact should be objectively measured are unauthorized access, unauthorized changes to data, unauthorized deletion of data, partial or complete loss of system availability, etc.

## 5.3 Likelihood

Given a threat, its likelihood measures the probability that the threat will occur “and” cause damage. Likelihood can be a qualitative description too. It should ideally combine the chance of the threat event being initiated and the chance that an initiated threat results in an adverse impact.

## 5.4 Risk Vulnerability

Risk vulnerability is a measure of the net harmful consequence of a given threat. It is measured by considering both the likelihood as well as the Impact of the given threat and calculated as below:

Risk = Impact \* Likelihood (where \* indicates multiplication)

## 5.6 Risk Assessment

A risk assessment is an exercise of making a list of all possible threats posed to the organization in the context of fulfilling its commitments to its customers and other stakeholders. It also measures the computed risk for each threat using the abovementioned method. Finally, the exercise benchmarks the computed risks against a predetermined acceptable risk level. Those threats above the acceptable level need to be addressed via mitigation measures.

## 5.7 Risk Management

Risk management is the program that implements risk assessment as described above and mitigation measures. It includes recognizing threats and risks, analyzing their likelihood and impact, treating and mitigating their outcomes, and monitoring the mitigation measures.

# 6. Risk Assessment Policy

- All Superhawk AI employees and contractors are responsible for identifying, analyzing, evaluating, monitoring, and communicating risks associated with any activity, function, or process within the scope of their responsibility and authority.
- Any employee or contractor who spots a potential risk or vulnerability should report it to the Information Security Officer or via the designated incident/risk reporting channel.
- All personnel are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible.
- The development and execution of risk assessments is the joint responsibility of the CEO, the Information Security Officer, and the department or individuals responsible for the area being assessed.
- Superhawk AI performs periodic risk assessments using qualified internal staff and, when required, external third parties with experience assessing SaaS/cloud environments and GDPR/SOC 2/ISO 27001 requirements.
- Risk assessment deliverables include a risk assessment report and a risk reduction



action plan that assigns risk owners, timelines, and acceptance criteria to manage or mitigate unacceptable risks. - The risk assessment process and methodology will be updated as required in response to audit findings, incidents, regulatory changes, and management direction. - Management defines the scope of each risk assessment and assembles the assessment team with a designated risk assessment lead. - Given the scope, the assessment team inventories assets, lists potential risks and threats to the system, and documents existing controls (including vendor-managed controls for AWS, GCP, GitHub, and Google Workspace). - For each threat, the impact is quantified on a relative scale of 0 to 10, where 0 indicates minimal impact and 10 indicates maximum impact. - For each threat, the likelihood is estimated as a number between 0 and 1. - The net risk of each threat is computed using the above two metrics. Net risk ranges between 0 and 10. The assessment will propose controls and actions to reduce impact and/or likelihood. - The assessment team creates a risk assessment report and communicates findings to management and affected teams; remediation tasks are assigned in the company's tracking system. - Risk mitigation actions are tracked to completion and their effectiveness is monitored and validated through follow-up reviews. - Risk assessments will be performed at least annually and additionally when significant changes occur (e.g., major product changes, cloud architecture changes, new regulatory requirements, or vendor changes). - Lessons learned from previous assessments and incidents will be incorporated into subsequent assessments to improve threat identification and controls.

## 7. Risk Mitigation

- When the net risk amounts to less than 3, there are very reasonable grounds to deem the risk acceptable.
- For higher risk values, the risk can still be considered acceptable if the cost of implementing mitigation measures exceeds the net dollar impact that might arise from the risk.
- If the risk cannot be mitigated, and the net risk exceeds 8, consider purchasing insurance as a protection measure. Consider the net dollar impact that might arise from the risk to evaluate the amount of insurance coverage.
- Threats/Risks shall be ranked in descending order of the net computed risk. This indicates the order of importance in which to address the threats. Controls are designed for the risks that have been selected to mitigate. A plan is created to implement the controls in this order.
- We then compute the "Residual risk" after fully implementing controls and mitigation strategies. One of the following decisions is made based on the residual risk:
  - Accept the risk.
  - Transfer the risk.
  - Add more controls.
  - Other actions as may be deemed necessary
- When the risk assessment report is completed, results shall be communicated to the affected business units and staff.

## 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 is responsible for approving and reviewing policy and related procedures. The Information Security Officer, together with the CTO and department leads, is responsible for coordinating risk assessments, assigning risk owners, and ensuring remediation tracking. Employees, contractors, and team leads are responsible for reporting risks, participating in assessments, and implementing assigned mitigation actions. External vendors remain responsible for controls they manage as specified in vendor contracts.

## 11. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization or technology stack (for example changes in AWS/GCP usage, GitHub workflows, Google Workspace configuration, or applicable legal/regulatory requirements such as GDPR).

---

End of Risk Assessment & 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 |