



Incident Management Policy

Version 1 - Approved by Rishabh



Contents

1. [Objective](#)
2. [Scope](#)
3. [Policy Statement](#)
4. [Information Security Incident Management](#)
5. [Document security classification](#)
6. [Non-Compliance](#)
7. [Responsibilities](#)
8. [Schedule](#)
9. [Version History](#)



1. Objective

The objective of this policy is to provide a framework within which information security events and incidents associated with information systems are communicated in a timely manner and necessary corrective actions are taken.

2. Scope

This document is applicable to all employees, contractors, and systems that process, store, or transmit Superhawk AI data and information within the scope of the ISMS. It covers cloud-hosted services and resources used by Superhawk AI, including AWS and GCP, code repositories in GitHub, and user accounts provisioned through Google Workspace, as well as employee devices (laptops/workstations) that access corporate resources.

3. Policy Statement

Security incidents are irregular and anomalous conditions that cause — or may lead to — service degradation, loss of sensitive data, outages, or any form of reduced operational status. These situations require quick human intervention to avert disruptions or restore the operational status.

This document offers guidance and establishes methods for handling and managing incidents for the staff or incident responders who believe they have discovered or are responding to a security incident.

4. Information Security Incident Management

4.1 Responsibilities and Procedures

- An Incident management procedure shall be created to define procedures and responsibilities to ensure quick, effective, consistent, and orderly responses to information security incidents.
- There shall be responsible personnel appointed for:
 - Ensuring that all employees, contractors, customers, and third parties are aware of incident reporting and communication channels.
 - Investigation/coordination of the reported information security incidents and security weaknesses.
 - Tracking closure of incidents and corrective and preventive actions.

4.2 Reporting Information Security Events and Incidents

- Superhawk AI's management shall establish and maintain incident reporting channels including an internal incident ticketing system (e.g., GitHub Issues or an equivalent tracking tool) and a dedicated incident response email alias within Google Workspace for initial notifications.
- All information security incidents shall be recorded in the company's incident tracking system. For incidents affecting cloud resources, responders shall capture relevant cloud



provider identifiers and logs from AWS and GCP as part of the record.

- The details of the steps to be followed for reporting an incident shall be communicated to all employees and contractors through onboarding materials and the internal wiki or documentation site.
- Incident reporting and management procedures shall be made available for easy access and reference for reporting security incidents and weaknesses by the users.
- A monitoring mechanism shall be set up for proactive monitoring of intrusions, attacks, and frauds using cloud provider logging and monitoring services (e.g., AWS CloudWatch, GCP Cloud Logging) and any security monitoring tools adopted by the company.

4.3 Assessment of and Response to Information Security Incidents

- All information security incidents that are reported shall be assessed and classified according to criteria defined in the incident management procedure, considering impact to PII, business data, behavioral data, service availability, and legal or contractual obligations (including GDPR).
- The assessment and classification of incidents shall be maintained for future reference to allow easy identification and avoid false positives.
- A response plan and strategy for the appropriate handling of security incidents shall be formulated, which covers the incident cycle from identification to root cause analysis to resolution, including steps for containment, eradication, recovery, and evidence preservation. For cloud-hosted assets, the plan shall reference cloud provider capabilities for snapshots, log exports, and access audit logs.
- Incidents should be communicated to the users impacted as per the legal, regulatory, and contractual agreements.
- The overall response to reported incidents shall include the identification of corrective action where important.
- Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction.

4.4 Learnings from Security Incidents

- The analysis shall be carried out for the information security incidents and shared with the appropriate authorities and internal stakeholders periodically. Post-incident reviews (post-mortems) shall be documented in the internal knowledge base and used to update controls and procedures.
- Knowledge gained from the resolution of security events shall be used to reduce the likelihood of similar incidents in the future and help limit the impact of the incident.

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. The Information Security Officer, together with the Engineering Lead and IT Administrator, shall maintain incident response readiness, ensure incident records are retained in the incident tracking system, and coordinate communications with affected parties and regulators (including GDPR-related notifications). Department heads and contractors are responsible for reporting incidents promptly and cooperating with investigations. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

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

End of Incident 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