Data Breach Notification Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

The objective of this policy is to outline the guidelines for notifying individuals, regulatory authorities, and other relevant parties in the event of a data breach. The policy aims to ensure prompt and appropriate actions are taken to mitigate the impact of a data breach, uphold the privacy and security of individuals' data, and comply with applicable laws and regulations.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who handle Personal Identifiable Information (PII), Business & Operational Data, or Behavioral Data collected, processed, or stored by the organization, including data stored in cloud platforms (AWS, GCP), on employee devices, and in third-party services used by the company.

3. Policy Statement

At Superhawk AI, we are committed to safeguarding the data that we collect for the delivery of our services. If sensitive data is acquired, accessed, used, or disclosed in a manner not permitted under the privacy law or in a manner that compromises the security or privacy of the sensitive data (personal data or PHI), it may be considered a Breach.

Data breach notification procedures shall be created to define procedures and responsibilities to ensure a quick, effective, consistent, and orderly response to Information Security Incidents that lead to a Data breach.

4. Reporting of Suspected Breach

Any Superhawk AI staff member, contractor, or authorized third-party who discovers a potential breach of Personal Identifiable Information (PII), Business & Operational Data, or Behavioral Data shall report it immediately to the company’s Information Security Officer via the designated incident reporting channel (email to the Information Security Officer and creation of an incident ticket in the company’s incident tracking system). If the Information Security Officer is unavailable, reports shall be escalated to the CTO.

5. Investigation of Suspected Breach

The Information Security Officer shall promptly review the circumstances of the suspected breach, coordinate evidence collection (logs from AWS/GCP, GitHub access records, and device information), and determine whether the incident was intentional or unintentional. The review will include a documented risk assessment of potential harm to data subjects and customers. Certain unintentional incidents that meet the criteria below do not constitute reportable breaches:

1. If Personal Identifiable Information (PII) was accessed or used by an employee or contractor of Superhawk AI in good faith and within the scope of their permitted duties, with no further unpermitted use or disclosure, this does not constitute a breach.

2. If PII was inadvertently disclosed by one staff member to another staff member without any further unpermitted use or disclosure, this does not constitute a breach.

3. The Information Security Officer shall document the risk assessment and, if the assessment concludes the incident could cause a significant risk of financial, reputational, or other harm to customers or data subjects, proceed with notification as described in Section 6.

6. Breach Notification to the customer

In the case of a sensitive customer data breach affecting PII or other regulated personal data, the Information Security Officer shall, without undue delay and where feasible no later than 72 hours after becoming aware, notify the competent supervisory authority in accordance with applicable laws (including GDPR) unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Notifications to affected customers will be coordinated with legal counsel and sent via the customer's registered contact method (email or account notification).

Where notification to the supervisory authority is not made within 72 hours, the notification shall include reasons for the delay and the results of the risk assessment.

Mitigation

Superhawk AI shall mitigate, to the extent practicable, any harmful effect known to the company resulting from unauthorized use or disclosure of sensitive data. Mitigation actions may include revoking compromised credentials, applying access changes in AWS/GCP, resetting user sessions, engaging impacted customers with remediation steps, and coordinating with third-party vendors to address vendor-managed controls.

7. Document Security Classification

Company Internal. Please refer to the Data Classification Policy for more details.

8. 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.

9. Responsibilities

The Information Security Officer is responsible for approving and reviewing this policy and related procedures, leading breach investigations, performing risk assessments, coordinating notifications to supervisory authorities and affected customers, and maintaining incident records. The CTO shall serve as the escalation point if the Information Security Officer is unavailable. System owners, DevOps engineers, and service admins shall provide required logs and access controls from AWS, GCP, GitHub, and employee devices as requested during investigations. Legal counsel and the

Data Protection Officer (where appointed) shall be consulted for regulatory and customer communication.

10. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization's infrastructure, data processing activities, applicable law (e.g., GDPR changes), or vendor relationships (e.g., onboarding or removal of cloud providers or major SaaS vendors).

End of Data Breach Notification 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