Encryption Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

Encryption is a process in which data is encoded so that it remains hidden from or inaccessible to unauthorized users. It helps securely protect data that you do not want anyone to access. By encrypting our data at rest and in transit, we can better protect private, proprietary, or critical data and enhance communication security between client applications and servers. This policy provides the guidelines to follow for the encryption of data.

2. Scope

This policy applies to all systems, services, and personnel that store, process, or transmit Superhawk AI's customer and business data. It covers cloud-hosted infrastructure and services (including AWS and GCP), code repositories (GitHub), employee devices (laptops/workstations), and third-party SaaS services used to support Superhawk AI's SaaS product and business operations. The scope includes production and non-production environments where sensitive data may be present.

3. Policy Statement

The purpose of this policy is to ensure the security of data at rest and data in transit for Superhawk AI. Data at rest refers to physically stored data, which is encrypted using various tools and managed by the infrastructure provider. Data in transit, actively moving between locations, also needs to be encrypted using TLS and trusted security certificates. Passwords and cryptographic keys need to be encrypted and stored securely. Rolling one's own cryptography is strongly discouraged.

4. Encryption Guidelines

4.1 Encryption at Rest

- Data at rest is defined as data that is physically stored and not actively moving from one location to another (i.e., device to device or network to network). This includes data stored on laptops, flash drives, and hard drives.
- Superhawk AI relies on cloud provider-managed encryption for data at rest. For data stored in AWS and GCP services (including managed databases and object storage), encryption at rest is enabled using the providers' native encryption mechanisms (e.g., AWS KMS, GCP Cloud KMS) with provider-managed keys by default. For employee laptops and workstations, disk encryption is enforced as described in the Endpoint Security Policy.

4.2 Encryption in Transit

- Data in transit is defined as data that is actively moving from one location to another (i.e., device to device or network to network). This includes data transferred over public networks such as the Internet. Superhawk AI encrypts data in transit using a variety of tools, including:
    - TLS: Always use HTTPS, SSL enabled (minimum standard is TLS v1.2).

    - Use security certificates provided by a known, trusted provider for all of Superhawk AI's public-facing properties on the Internet.
- Internal service-to-service communication in cloud environments must use TLS with modern ciphers (TLS 1.2 or higher). Connections to third-party services (e.g., GitHub, Google Workspace) must use their provided encrypted channels (HTTPS, TLS).

4.3 Rolling Your Own Crypto

Please don't roll your own crypto. If you really think you have a situation where it makes sense to do this, please don't. If you're absolutely sure you have an edge case where this makes sense, please contact the Information security officer so they can work with you on finding an alternative.

4.4 Password Encryption

All user and customer passwords stored by Superhawk AI must be hashed using a strong, adaptive one-way algorithm (e.g., bcrypt, Argon2) with appropriate work factors; plain-text storage is prohibited. Passwords must be transmitted over encrypted channels (TLS). Secrets used by services (API keys, service account credentials) shall be stored in cloud-managed secret stores (e.g., AWS Secrets Manager, GCP Secret Manager) or an approved secrets management solution.

4.5 Cryptographic Keys

Cryptographic keys and secrets shall be generated using secure library functions and stored in managed key management services (e.g., AWS KMS, GCP Cloud KMS, or an approved HSM-backed service). Access to keys shall be restricted by IAM policies and audited. Local persistent storage of master keys is prohibited; rotation and lifecycle management of keys shall follow the Key Management procedures.

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. Cloud infrastructure owners (AWS/GCP) and platform engineers are responsible for configuring and validating provider-managed encryption. Engineering teams are responsible for implementing password hashing and

using approved secrets management. All employees, contractors, and third-party vendors must comply with this policy when handling Superhawk AI data.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization or its use of cloud providers, code repositories, or third-party services (e.g., onboarding AWS/GCP features or replacing GitHub/Google Workspace integrations).

End of Encryption 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