Communications & Network Security Policy

Version 1 - Approved by Rishabh

Contents

1. Objective
2. Scope
3. Policy Statement
4. Communication & Network Security
5. Document Security Classification
6. Non-Compliance
7. Responsibilities
8. Schedule
9. Version History

1. Objective

Superhawk AI shall take adequate precautions and design appropriate controls to prevent misuse of its information assets and information processing facilities. In this regard, Superhawk AI shall establish necessary communication and network security procedures, protect information in networks and support infrastructure, maintain the security of information being transferred, and detect any unauthorized information processing activities.

2. Scope

This document applies to all employees, contractors, and systems that store, process, or transmit Superhawk AI data within the scope of the Information Security Management System, including cloud infrastructure hosted on AWS and GCP, developer code repositories on GitHub, and corporate accounts within Google Workspace. It covers corporate networks, remote connections from employee devices (laptops/workstations), and any integrations with third-party SaaS services handling Personal Identifiable Information (PII), business & operational data, and behavioral data.

3. Policy Statement

Superhawk AI is committed to ensuring the highest level of service to its customers. Consequently, it is paramount to manage and control networks to protect them from threats and maintain the security of their systems and applications.

4. Communication & Network Security

4.1 Network Security Management

4.1.1 Network Controls

- Networks shall be adequately managed and controlled to be protected from threats and to maintain the security of the systems and applications using the network, including information in transit.
- Network-based intrusion prevention/detection system shall be deployed, wherever possible, to cover critical network segments within IT infrastructure.
- Infrastructure elements and software(s) exposed to un-trusted or semi-trusted networks/users (e.g., Internet-facing systems, distributors, call centers, Contract Partners, etc.) shall be adequately protected by firewalls, Intrusion Prevention Systems (IPSs), and limited connectivity and encryption.
- Any system deployed on the Internet must go through a thorough vulnerability check.
- All configurations must be done by trained and authorized personnel. Any changes to network configurations should follow the Operations Security Procedure.
- Vulnerability assessment of these infrastructure elements shall be carried out every year.
- All end-user systems connecting to the Superhawk AI infrastructure should have baseline security implemented.
- Where network and infrastructure services are provided by cloud providers (AWS and GCP) or third-party SaaS vendors, Superhawk AI shall rely on the providers' managed controls for

underlying physical and hypervisor-level security; Superhawk AI remains responsible for secure configuration, network segmentation, firewall rules, and encryption settings within those cloud environments.

4.1.2 Information Transfer Policies & Procedure

- Users shall be made aware, and information transfer guidelines shall be captured in the Data Classification Policy and Asset Management procedure, and users shall be made aware of these guidelines.
- Acceptable use standards shall be established to define guidelines for the appropriate use of communication facilities.
- Appropriate anti-malware controls shall be established to detect and prevent malware that could be transmitted through electronic communication channels.
- Employees shall treat all correspondence sent using Superhawk AI email systems as confidential.
- To prevent loss, modification, destruction, or misuse of information, Superhawk AI shall protect and control the exchange of critical business information assets and software with third parties and outside organizations.
- Where feasible, it is recommended to consider the implementation of appropriate web filtering mechanisms that will restrict user access to external networks and websites based on the organization's policies.
- Data transfers involving PII or other sensitive data to or from third-party services must be performed over encrypted channels (e.g., TLS) and documented in vendor assessments; transfers to cloud storage or processing services on AWS/GCP must follow approved configuration baselines and access controls.

4.1.3 Electronic Messaging

- Information involved in electronic messaging (e.g., emails, instant messengers) shall be appropriately protected from unauthorized access, modification, or denial of service.
- Public email accounts shall not be used for conducting Superhawk AI operations unless authorized.
- Forwarding of Superhawk AI mailbox to public or non-Superhawk AI email accounts shall be done in accordance with the Data Classification policy.
- Corporate email and messaging are provided via Google Workspace; security configurations (including MFA enforcement, secure transport (TLS), and DLP rules where applicable) shall be maintained in Google Workspace by IT/InfoSec.

4.1.4 Confidentiality or Non-Disclosure Agreements

- Confidentiality or non-disclosure agreements reflecting Superhawk AI needs for the protection of information shall be identified and maintained with all the third parties, and this will be based on the criticality of the information to be protected. These requirements shall be reviewed at least once a year and at the time of any change in the business environment, legal requirements, and contractual obligations.
- Confidentiality and non-disclosure agreements shall comply with all applicable laws and regulations for the jurisdiction to which they apply.

- Both staff members and contract partners of Superhawk AI shall sign and comply with the non-disclosure agreement (NDA) that is established and maintained by the Superhawk AI's HR team, where applicable.
- Vendor relationships that involve processing PII, business, or behavioral data (including cloud providers AWS/GCP and code repository provider GitHub) shall require documented data processing agreements or equivalent contractual terms that meet GDPR and SOC 2 requirements.

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. The IT team is responsible for managing cloud network configurations and firewall rules in AWS and GCP; DevOps and engineering maintain secure configurations for services deployed from GitHub repositories. HR shall manage NDAs for employees and contractors. All employees and contractors must follow this policy and report security incidents to the Information Security Officer.

8. Schedule

This document shall be reviewed at least annually and additionally when significant changes occur, such as onboarding new cloud providers, major changes in data processing practices, or changes in applicable regulatory requirements (e.g., GDPR, SOC 2 scope).

End of Communications & Network Security 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