Network Security Procedure

Version 1 - Approved by Rishabh

Contents

1. Objective

Network security shall help minimize information security risk to a great extent and protect the organization against the threat of unintended information disclosure. Superhawk AI networks (includes Cloud, VPC, and cloud services) must be protected from internal and external intrusion by designing network security at a level that is appropriate for the nature of data transmitted to protect all business data, related application systems, and operating systems software from unauthorized or illegitimate access. It is imperative to establish controls that protect Superhawk AI networks against information security threats.

The primary use of this document is to provide guidance for implementing Network Security controls.

2. Scope

This procedure applies to all employees, contractors, and systems involved in the operation, maintenance, or access of Superhawk AI's networked environments that are in scope of the ISMS. It covers cloud infrastructure hosted on AWS and GCP, virtual networks (VPCs), and network-related configurations in third-party SaaS services (e.g., Google Workspace) as they pertain to transmission or storage of PII, business/operational data, and behavioral data.

3. Network Security Management

3.1 Network Control

- The Engineering team shall designate named employees for managing Superhawk AI network environments in AWS and GCP, and for oversight of network-related configurations in third-party services such as Google Workspace.
- Where applicable, Web Application Firewalls (WAF) provided by cloud providers (for example AWS WAF, Google Cloud Armor) should be configured to log protocol anomalies, provide traffic analysis, and alert on system malfunctions.
- All network configuration changes must follow the company's change management process and be recorded in the change log (for example via GitHub for IaC changes and the change ticketing system used by Engineering).
- Network and security device logs (cloud provider logs, WAF logs, VPC flow logs, and relevant SaaS audit logs) shall be collected and monitored by the Engineering or Security team using available cloud-native services (e.g., AWS CloudWatch, GCP Logging) or a designated logging/monitoring tool.
- Any anomaly detected is raised as an information security incident through proactive monitoring, wherever applicable and implemented (examples include AWS Guard Duty or Microsoft Defender etc.).
- The Engineering Head shall ensure that sensitive data transmitted across networks is protected using appropriate encryption in transit (for example TLS) and that cloud provider-managed encryption features are enabled where applicable.

3.2 Security of Network Services

- The Engineering department should identify the security requirements for the network. These include requirements such as, but not limited to:
    - Encryption;
    - Intrusion detection and prevention system; and
    - Network monitoring.
- The Engineering team shall ensure identified network security requirements are implemented for AWS and GCP resources under Superhawk AI's control, and that relevant configurations for third-party SaaS (e.g., Google Workspace) meet these requirements.
- When network services are provided by third parties, contractual agreements must include the required security controls and data protection obligations.
- The Information Security Officer together with the Engineering team shall ensure a third-party independent network assessment (or cloud configuration assessment) is performed at least annually; this may be part of a VAPT engagement.
- Assessment results shall be documented and communicated to Engineering for remediation within agreed timelines.
- Following remediation, Engineering shall perform follow-up testing or validation to verify that identified issues have been addressed.

3.3 Network Access Control

3.3.1 Use of Network Services

- Access to production networks and cloud management consoles shall be restricted to authorized personnel based on role and least privilege principles.
- A maintained inventory of users with access to production network resources and cloud management interfaces shall be kept; where possible this inventory should be generated from identity and access management systems (e.g., AWS IAM, GCP IAM, Google Workspace Directory) and supplemented manually if automated generation is not available.
- The Information Security Officer and Engineering Head shall review and certify access to production network resources at least quarterly.

3.3.2 Remote Diagnostic & Configuration Port Protection

All remote access to infrastructure should be configured in a manner such that diagnostic and configuration services are accessible through a dedicated in-band management network interface, over an encrypted application layer protocol such as SSL or SSH only.

3.3.3 Segregation of Networks

- Networks shall be segregated using cloud-native VPCs/subnets and security controls in AWS and GCP to separate production, development, and testing environments.
- Data flow between network domains shall be controlled via secure gateways, firewalls, and cloud routing rules.
- Public subnets and bastion/jump hosts shall be configured to allow access to production or development environments based on role-based access controls and just-in-time access where appropriate.

- The Engineering Team is responsible for granting and revoking access to production and development environments according to defined roles and responsibilities.

3.3.4 Remote Devices

- All company-managed laptops and workstations that access production infrastructure must run supported endpoint protection software with up-to-date signatures and OS security patches.
- Users connecting from public networks are required to use approved remote access mechanisms (for example VPN or cloud provider secure access methods) and to ensure host firewalls are enabled.

4. Document Security Classification

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

5. 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.

6. 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.

7. Schedule

This document shall be reviewed annually and additionally whenever significant changes occur to cloud infrastructure (AWS or GCP), network architecture, or applicable regulatory requirements (SOC 2, ISO 27001, GDPR).

End of Network Security Procedure. 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