Acceptable Usage Policy

Version 1 - Approved by Rishabh

Contents

1. Objective

Superhawk AI is committed to safeguarding the data processed by its staff, software, or services. Our customers, partners, and other stakeholders depend on us to take appropriate measures to protect the data in our possession. Thus, each staff member needs to understand how to responsibly use our systems so that we appropriately safeguard the data in our possession.

2. Scope

This policy applies to all staff members, including employees, contractors, consultants, temporary workers, and interns who access or manage Superhawk AI systems and data. It covers use of company-issued devices and accounts, personal devices when used to access Superhawk AI systems, and company-administered third-party services.

Specifically, this policy applies to:

- Company-issued electronic, computing, storage, or network devices. - Personal devices (laptops, workstations, mobile devices) when used to access company resources, including Google Workspace and GitHub. - Company-owned systems and services hosted on cloud platforms (AWS, GCP) and any company-administered accounts with third-party services.

3. Policy Statement

Superhawk AI has a culture of trust and integrity. This policy aims to reinforce the trust we place in each other by ensuring we can collectively depend on each other to protect the assets of our staff, company, partners, and customers.

Security is a company-wide effort and requires cooperation from every staff member who works with Superhawk AI systems. Individuals should take precautions to ensure they use systems appropriately and not deliberately or inadvertently perform destructive or illegal actions.

4. Separation of Concerns

Company-issued devices and accounts are not personal property, so limiting their use for personal reasons is strongly recommended.

5. Security of Critical Data

- All data stored on computing and storage devices, whether owned or leased by Superhawk AI, the employee, or a third party, and all data stored in cloud platforms (AWS, GCP) used by Superhawk AI, remains the sole property of Superhawk AI.
- All critical data must be handled and secured in accordance with the Data Classification Policy and relevant procedures for cloud-hosted data and endpoint devices.
- Staff must promptly report theft, loss, or unauthorized disclosure of any critical data to Security and People Operations through the incident reporting process.

- Access to, use of, or sharing of critical data is permitted only to the extent authorized and necessary to perform assigned job responsibilities; access to code repositories is managed via GitHub access controls and roles.
- Staff are responsible for exercising good judgment when using Superhawk AI systems for reasonable personal use; where unsure, staff must consult their manager or People Operations.
- Superhawk AI reserves the right to audit systems and to monitor equipment, services (including Google Workspace, GitHub), and network activity to ensure compliance with this policy, subject to applicable law and privacy obligations (including GDPR).

6. Unacceptable Use

Staff members may not use Superhawk AI-managed resources for activities that are illegal or prohibited under applicable law, no matter the circumstances.

6.1 Unacceptable System & Network Activities

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations.
- Unauthorized copying, distribution, or use of copyrighted material.
- Exporting software, technical information, encryption software, or technology in violation of international or national export control laws.
- Intentional introduction of malicious programs into Superhawk AI networks or any Superhawk AI-managed computing device.
- Intentional misuse of any Superhawk AI-managed computing device or networks (e.g., for cryptocurrency mining, botnet control, etc.).
- Sharing credentials for any Superhawk AI-managed computer or third-party service (including Google Workspace and GitHub) with others, or allowing others to use your account. This prohibition does not apply to approved single-sign-on technologies.
- Using a Superhawk AI computing asset to procure or transmit material that violates sexual harassment policies or creates a hostile workplace.
- Making fraudulent offers of products, items, or services originating from any Superhawk AI account.
- Intentionally accessing data or logging into a computer or account that the staff member is not authorized to access, or disrupting network communication or computer processing.
- Executing network monitoring that intercepts data not intended for the staff member’s computer, except when authorized for troubleshooting or security purposes.
- Circumventing user authentication or security of any computer host, network, or account used by Superhawk AI.
- Tunneling between network segments or security zones, except when authorized for troubleshooting or security activities.

6.2 Unacceptable Email & Communications Activities

- Forwarding confidential business emails or documents to personal external email addresses (including personal Google accounts) without authorization.

- Note: Superhawk AI may retrieve messages from archives and servers without prior notice if Superhawk AI has sufficient reason to do so. If deemed necessary, this investigation shall be conducted with the knowledge of the Information Security Officer, Senior Management, People Business Partners, and the Legal team.

6.3 Return of Superhawk AI-Owned Assets

All Superhawk AI-owned computing resources, including laptops, mobile devices, access tokens, and company accounts, must be returned or access revoked upon separation. Staff must remove any personal data only after complying with company offboarding procedures; IT and People Operations will verify asset return and account termination.

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. People Operations is responsible for communicating the policy during onboarding and offboarding. Engineering and IT (platform) teams are responsible for implementing technical controls (GitHub access management, cloud IAM on AWS/GCP, and Google Workspace configuration). All staff are responsible for complying with this policy and reporting incidents.

10. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization, such as adoption of new cloud providers, major changes to third-party services (e.g., Google Workspace, GitHub), or changes to applicable regulatory requirements (SOC 2, ISO 27001, GDPR).

End of Acceptable Usage 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