



Access Control Procedure

Version 1 - Approved by Rishabh



Contents

1. [Objective](#)
2. [Scope](#)
3. [Access Control Procedure](#)
4. [Document Security Classification](#)
5. [Non-Compliance](#)
6. [Responsibilities](#)
7. [Schedule](#)
8. [Version History](#)



1. Objective

The objective of this document is to establish a procedure and framework for user access management and controlling access to assets and information systems of Superhawk AI, in accordance with the Access Control Policy.

2. Scope

This procedure applies to all employees, contractors, and third-party users who require access to Superhawk AI's information systems and cloud infrastructure, including AWS and GCP, code repositories (GitHub), Google Workspace, and any other systems classified as critical.

3. Access Control Procedure

3.1 Requirements for Access Control

- A list of systems that are critical from an access control standpoint is listed and maintained in the Sprinto App. Superhawk AI the Information security officer is responsible for maintaining this list up to date.
- A list of all critical systems that require access control shall be made available in the Sprinto App in one of the following ways:
 - Integrated Systems – Where possible, the respective administrators of critical systems should integrate the system with Sprinto App for automated and continuous monitoring of access control requirements. Examples of such systems include cloud infrastructure providers (like AWS, Azure), version control systems (like Github, Bitbucket), email providers (like Google Workspace, Microsoft O365), HRMS systems, etc.
 - Monitored Systems - Where integrations are not possible, the critical systems should be added to Sprinto App for tracking and monitoring. Adding such systems to Sprinto App to ensure they are monitored is the responsibility of the Information Security Officer.
- It is the responsibility of the Information Security Officer to ensure that the roles that can get access to each critical system are configured in the Sprinto App.

3.2 Access Provisioning

- The access to Superhawk AI systems should be initiated only after an offer letter, including the terms and conditions of employment, has been formally signed by the employee.
- By default, all employees get access to systems that are configured to be given to all staff. Examples include email providers or internal messaging tools.
- Access to other systems is assigned by respective system administrators based on the organization's role matrix after onboarding; for code and infrastructure access this includes GitHub, AWS, and GCP administrators following least-privilege assignments.
- Users who are not configured to have access to a particular system will be automatically monitored and alerted by Sprinto App. It is the responsibility of the Information Security



Officer to respond to such alerts and ensure the role matrix is updated or the access is removed.

- For Integrated systems, the Information Security officer should ensure that User IDs created in the systems for each user are tagged to their respective company email IDs in the Sprinto App to ensure users are identified and tracked continuously.
- For access provisioning of third-party users (consultants, auditors, vendors and suppliers, etc.), the Information Security Officer or the relevant business head must approve access requests. System administrators must implement time-bound access and ensure accounts are disabled when no longer required.

3.3 Management of Privileged Access Rights

- It is the responsibility of system administrators to ensure that the least privilege principle is followed when granting access.
- As a part of access reviews, the Information Security Officer shall coordinate with system administrators and business owners to review and document privileged accounts (including AWS/GCP console, GitHub organization admins) and approve or revoke privileges as needed.

3.4 Management of Secret Authentication Information of Users

- Where possible, SSO and MFA need to be enabled to reduce reliance on passwords.
- For critical systems that are integrated with the Sprinto App, it is the responsibility of the Information Security Officer to ensure the MFA status for users with access to systems is monitored continuously on the Sprinto App.
- In case of discrepancies alerted by Sprinto App, the Information Security Officer should ensure corrective actions are taken immediately.
- For Monitored Systems, the Information Security Officer should make sure that secure login/password management is enabled and that the evidence for it is uploaded on the Sprinto App.

3.5 Review of Access Rights

- Access reviews should be carried out quarterly for production systems (including AWS, GCP, GitHub, and Google Workspace) and at least annually for non-production systems. Reviews will be led by the Information Security Officer with input from system administrators and business owners.
- The access review for critical systems should be completed within the Sprinto App where possible. For all monitored systems, evidence of performing reviews needs to be uploaded to the Sprinto App.
- Any corrective action that needs to be taken in case of discrepancies noted should be documented as a part of the access review activity.
- Review of access rights should also include reviews of privileges assigned to individual users to ensure segregation of duties.

3.6 Removal or Adjustment of Access Rights



- In case of any termination or change in role, the HR team (or authorised HR representative) must notify system administrators, managers, and the Information Security Officer immediately to revoke or modify access.
- On termination of employment, access revocation from all critical systems should be completed within three days from the employee's last working day.
- In case of a change in role, the HR team shall verify and update role assignments in the HRMS and Sprinto App, notify administrators to adjust system access, and inform the Information Security Officer to update the role-based access matrix.

3.7 User Responsibilities

- Users are responsible for following the organization's access control policy and procedure.
- Users are responsible for keeping their passwords confidential.
- Users are responsible for changing the passwords whenever there is any indication of possible system or password compromise.
- Incidents relating to passwords or personal authentication information sharing must be reported to the Information Security Officer via the company incident reporting channel (e.g., Google Workspace email to the security mailbox) and logged in the incident tracking system.
- Users shall not leave their system unattended while logged on. They shall lock the system even if they are moving away from the system for a short period of time.

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. System administrators for AWS, GCP, and GitHub are responsible for enforcing least-privilege access and providing evidence for access reviews. HR is responsible for notifying changes in employment status.

7. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization or its cloud infrastructure, tooling (e.g., GitHub, Google Workspace), or applicable regulatory requirements (SOC 2, ISO 27001, GDPR).



End of Access Control 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