HR Security Procedure

Version 1 - Approved by Rishabh

Contents

1. Objective

This procedure specifies the information security requirements that should be considered throughout the various stages in the Human Resource lifecycle of employees (full-time and part-time) and external parties, including contractors and other third-party staff, (as applicable), including pre-employment, during employment, and at the end of employment.

2. Scope

This procedure applies to all employees (full-time and part-time), contractors, and other third-party staff who have access to the organization's information systems, data, or physical assets. It covers HR activities that affect access, onboarding, offboarding, and personnel-related security controls for systems and data hosted on cloud platforms (AWS, GCP) and for organization-managed employee devices (laptops/workstations).

3. HR Security Procedure

3.1 Before Employment

- Before releasing the offer letter, the Head of People (People Operations) must ensure that potential employees are duly evaluated on their capability to perform the job role. This shall be documented as a hiring evaluation and is maintained after the employee has joined Superhawk AI.
- The Head of People (People Operations) should ensure that the offer letter which includes the terms and conditions for the employees has been signed by the employee.
- The Head of People (People Operations) must ensure that the Background Verification (BGV) of employees is initiated at the time of the joining and that the final Background Verification reports are documented and maintained.

3.2 During Employment

- Once the employee has joined, the Head of People must ensure that the user has been onboarded onto required cloud-based tools and systems (including Google Workspace and GitHub) and granted appropriate access as required, following least privilege principles.
- After an employee joins, the Head of People must assign them a role and reporting manager to make sure the organization chart is updated and documented. The list of active roles within the organization and their job descriptions also needs to be documented and maintained.
- Head of People should make sure that new joiners read and acknowledge organizational policies within 30 days of joining.
- Employees must also finish the information security awareness training. The status should be tracked in HR records or the learning platform, and Head of People must ensure Employees finish the training within 30 days of joining.
- The Information Security Officer or Head of People should send out periodic training requests and policy acknowledgment requests to all employees at least annually. The status

of completion can be tracked, and it is their responsibility to ensure all employees finish the periodic activities.
- Employees shall be evaluated by their reporting manager regarding their job and information security responsibilities at least once annually. These evaluations also need to be documented and maintained.

3.3 Termination or change in employment

- Once an employee decides to terminate his employment with Superhawk AI, the last working day must be decided in concurrence with the reporting manager and Head of People. The following processes need to be kickstarted on the last working day:
    - The Head of People or designated HR staff must ensure any company-owned asset or device is returned to the organization.
    - The user needs to be offboarded from all critical systems that they have been provided access to. For cloud services (AWS, GCP, Google Workspace, GitHub), access revocation shall be performed via the relevant admin consoles by the system administrators or delegated administrators.
    - Access to critical systems must be revoked within 3 days of the termination date; for privileged accounts this should be revoked immediately upon termination. The respective administrators need to be notified by the Head of People. The status can be tracked and monitored in the HR offboarding checklist.
    - In case any user access needs to be retained, HR must notify respective admins to change the password to such accounts and document the justification for the same.

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. The Head of People (People Operations) is responsible for executing HR lifecycle activities (hiring, onboarding, offboarding, and personnel records). System administrators and application owners (for AWS, GCP, Google Workspace, and GitHub) are responsible for provisioning and revoking access to systems and maintaining logs. Employees, contractors, and third-party staff are responsible for complying with this procedure and completing required trainings and acknowledgments.

7. Schedule

This document shall be reviewed annually or when significant organizational changes occur, such as changes to cloud providers (AWS, GCP), identity providers, or HR processes.

End of HR 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