HR Security Procedure

Version 1 - Approved by Shreyas Srinivas

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) and external parties, including contractors and other third-party staff (as applicable), having access to Inai Technologies Co information systems.

3. HR Security Procedure

3.1 Before Employment

- Before releasing the offer letter, the People Operations Head 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 are maintained after the employee has joined Inai Technologies Co.
- The People Operations Head should ensure that the offer letter which includes the terms and conditions for the employees has been signed by the employee.
- The People Operations Head 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 People Operations Head must ensure that the user has been onboarded onto all necessary tools and systems, granting them appropriate access as required.
- After an employee joins, People Operations Head 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 description also needs to be documented and maintained.
- People Operations Head should make sure that the 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, and the HR head must make sure that Employees finish the training within 30 days of joining.
- The Information Security Officer or the People Operations Head 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 atleast 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 Inai Technologies Co, the last working day must be decided in concurrence with the reporting manager and People Operations Head. The following processes need to be kickstarted on the last working day:
    - HR team 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 by the People Operations Head.
    - Access to critical systems must be revoked within 3 days. The respective administrators need to be notified by the People Operations Head. The status can be tracked and monitored.
    - 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 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, up to and including 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 should be reviewed annually and whenever significant changes occur in the organization.

End of HR Security Procedure. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Shreyas Srinivas	12 Mar, 2024
1	New Policy version Created	12 Mar, 2024