HR Security Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this policy is to provide a framework within which the information security requirements of human resources are addressed throughout the entire lifecycle of recruitment, employment, change of employment, and termination. CNTXT shall ensure that employees (full-time and part-time) and external parties, including contractors and other third-party staff, understand the responsibilities for the roles they are considered for and are aware of and fulfill their information security responsibilities. Additionally, CNTXT shall protect the company's interests while changing or terminating employment.

2. Scope

This policy applies to all employees (full-time and part-time) and external parties, including contractors and other third-party staff (including housekeeping staff and security personnel), with access to CNTXT information systems.

3. Policy Statement

CNTXT shall ensure that employees (both full-time and part-time) and external parties, including contractors and other third-party staff, understand their responsibilities for the roles they are considered for and are aware of and fulfill their information security responsibilities. Moreover, CNTXT shall also protect the company’s interests while changing or terminating employment.

4. Human Resource Security Guidelines

4.1 Before employment

- As part of the hiring process, the competence of all candidates considered for employment shall be evaluated to ensure that they can perform the expected job responsibilities.
- Once employed, all CNTXT employees and contract partners shall sign the terms and conditions of employment, which shall include the employee’s responsibilities for information security and related obligations, both during and after employment.
- Background verification checks shall be performed on all prospective employees where possible:
    - The extent of background verification checks will be proportional to business requirements, the classification of information to be accessed, and the perceived risks. This may include previous employment checks, confirmation of claimed academic and professional qualifications, identity checks, or criminal record checks for prospective CNTXT employees.
    - In specific geographies, background verification checks may be considered illegal. In such cases, you may consider conducting a reference check depending on the level of information

accessible to such employees.

- Considering privacy, protection of personal data, and other relevant employment laws and regulations that may be applicable, contract partners shall be assessed for their information security practices as part of the Vendor Risk assessment. For more details, please refer to the Vendor Management Policy.

4.2 During Employment

- Roles and responsibilities related to Information Security shall be defined and documented for all employees (full-time and part-time), contractors, and third-party staff where applicable.
- All employees, relevant contractors, and third-party staff shall receive appropriate awareness training on organizational policies and procedures, including security requirements, legal responsibilities, and other controls, such as understanding the acceptable use of CNTXT systems and the Code of Business Conduct at CNTXT.
- Awareness training on organizational policies shall also be conducted upon joining and at least once a year thereafter.
- Formal information security training shall be provided to employees upon joining and at least once a year thereafter.
- Organizational policies and the formal information security training deck shall be available to all employees on a public portal.
- The Information Security Officer shall be responsible for implementing and complying with information security controls by all employees.

4.3 Termination or Change in Employment

- Upon termination, CNTXT employees shall return/hand over the organization's assets under their purview.
- Upon termination, all access rights and privileges to critical information systems granted to employees or contractors shall be revoked according to the access control policy.
- In the case of a change in employment status, access rights and privileges to critical information systems granted to employees and contractors shall be reviewed and adjusted accordingly.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

6. 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.

7. 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.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

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

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024