Compliance Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this procedure is to establish the methods by which management of regulatory and legal compliance requirements for the systems which are in the scope of the Information Security Management System (ISMS) that is implemented.

2. Scope

This document is applicable to all processes and operations in CNTXT within the scope of the Information Security Management System (ISMS) (refer to the definition in Section 3 of the Information Security Policy).

3. Compliance with Legal Requirements

3.1 Identification of Applicable Legislation

- The Information Security Officer, along with the Legal team and the Engineering team, should be responsible for the identification of any legislation that might have an impact on the policies and procedures laid down. They should be guided by the CEO.
- Information Security Officer should update the applicable legislation as a part of the Information Security Manual and the associated procedures (Applicable and Mandatory only ISO 27001 is implemented).
- Advice on statutory, regulatory, and contractual requirements of CNTXT should be sought from the Engineering Team and the Legal team.
- The Information Security Officer, along with other relevant teams, should also ensure that all the required controls are implemented to ensure compliance.
- Regular periodic reviews of the compliance should be carried out by the Engineering team in conjunction with the Information Security Officer.

3.2 Data Protection & Privacy of Personal Information

- Data protection and privacy should be ensured as required in the identified relevant legislation, regulations, and applicable contractual clauses.
- The identified relevant legislation, regulations, and applicable contractual clauses should be communicated to all persons involved in the processing of personal information.
- The Information Security Officer should provide the necessary guidance to the Business Heads on their individual responsibilities and the specific procedures that should be followed.
- Any access to personal information should be on a “need-to-know” basis.

4. Safeguarding Organizational Records

All organizational records shall be managed in accordance with the Data Classification Policy.

4.1 Prevention of Misuse of Information Processing Facilities

Information processing facilities are to be used in accordance with the Acceptable Usage Policy.

5. Independent Reviews of Compliance with Security Policies & Standards

- Compliance with the following policies and procedures shall be continuously monitored:
  - Human Resources Security
  - Asset Management
  - Physical and Environmental Security
  - Communications and Operations Management
  - Systems Acquisition, Development, and Maintenance
  - Supplier Management
  - Access Control
  - Network Security
  - Security Incident Management
  - Compliance
- Information Security Officer should ensure that all security procedures are appropriately tracked in accordance with the defined procedures.
- The HR team should be responsible for educating employees regarding the security policies and associated procedures.
- Each department should regularly review the status of compliance within its area of responsibility. If any non-compliance is found as a result of the review, managers should:
  - Determine the causes of the non-compliance.
  - Evaluate the need for actions to ensure that non-compliance does not recur.
  - Determine and implement appropriate corrective action.
  - Inform the Information Security Officer if required.
- Information Security Officer should conduct a review once a year of all areas to ensure compliance with security policies and procedures.

6. Technical Compliance Checking

One annual technical assessment and review should be performed by a competent third-party along with the Engineering team to identify any potential vulnerabilities in the networks and other production systems. The findings of the assessment shall then be reported to the Information Security Officer.

7. Intellectual Property Rights

Care must be taken by the Engineering team and the Information Security Officer that all third-party software and services are appropriately licensed and do not violate any copyrights or intellectual property rights.

8. Information Systems Audit

8.1 Preparing & Conducting Audits

- While CNTXT has implemented an automated compliance monitoring tool that performs continuous monitoring of the control environment and effectiveness of adherence to policies and procedures, there should be an annual audit performed of the control environment to ensure compliance is maintained. The key things to consider in this audit are:
    - Completeness of inventory of assets and systems.
    - Adherence to procedure SLAs.
    - Review of the list of vendors.
    - Review of Information Security Risks.
- The audit may be performed by the Information Security Officer or an independent internal auditor, and the results must be communicated to the Senior management and should be reviewed by the senior management at least annually.

8.2 Audit Reports, Findings & Non-Conformance Closures

- The auditors should perform the audit and record the non-conformances and their observations/ suggestions in the Internal Audit Report.
- Any corrective actions that need to be taken must be documented in a corrective and preventive action (CAPA) register.
- The internal audit report, along with the CAPA register must be presented to the senior management for their review.
- The respective departments or functions should initiate corrective and preventive action on the non-conformances and close them within the committed closure time.
- At the end of the committed time frame, the Information Security Officer should verify the closure of the non-conformances.

9. Corrective & Preventive Actions (Applicable & Mandatory Only if ISO 27001 is Implemented)

The process for corrective/preventive action should be initiated whenever a condition warrants an investigation to determine if corrective or preventive action is required.

9.1 Corrective Actions

- Corrective action should be documented using the Corrective Actions, and Preventive Actions Register (CAPA Register) if a non-conformance is raised during the internal audit. Corrective action should be initiated as a result of, but not limited to, the following:
    - Non-conformances identified during internal audits or external audits.
    - Action items from management reviews of information security effectiveness.
    - Reported security incidents.
    - Reported deviations in the provision of services.
- Problems identified by employees pertaining to security weaknesses.
- Violation of security policy and security objectives.

9.2 Preventive Actions

- Information Security Officer should maintain a summary of the corrective and preventive actions taken. (The corrective and preventive action details should be maintained in the same summary sheet).
- Preventive action should be determined from the analysis of appropriate data to detect trends and identify causes that may result in future non-conformances.
- The Information Security Officer should verify the effectiveness of corrective/preventive action taken for the concerned departments.
- The results of corrective/preventive actions should be reviewed by the Senior Management during the meeting with the Information Security Officer.

10. Document Security Classification

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

11. 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.

12. 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.

13. Schedule

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

End of Compliance Procedure. 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