Compliance Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The purpose of this policy is to establish guidelines for the management of regulatory and legal compliance requirements for systems in accordance with applicable standards such as ISO 27001:2013, ISO 27001:2022, SSAE 18(SOC 2), and other standards.

2. Scope

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

3. Policy Statement

The information security management system of CNTXT shall be established and operated with due consideration for compliance with statutory, regulatory, or contractual obligations as well as any specific security requirements.

4. Compliance Policy

4.1 Identification of Applicable Legislations & Compliance Requirements

All relevant statutory, regulatory, and contractual requirements of the operations shall be explicitly defined and documented for CNTXT's information systems. The policies and procedures shall encompass and adhere to the applicable laws where applicable. Documentation of the requirements is mandatory only for ISO 27001. For other standards, ensuring compliance with the applicable requirements must be taken into account, but explicit documentation is not required.

4.2 Intellectual Property Rights

CNTXT shall comply with the terms and conditions and license requirements of copyrighted software, client intellectual property, or any other proprietary information used within the organization.

4.2.1 Protection of Organizational Records

CNTXT's records related to information security shall be protected from loss, destruction, and falsification in accordance with statutory, regulatory, contractual, and business requirements.

4.2.2 Data Protection and Privacy of Personal Information

Data protection and privacy shall be ensured as required by relevant legislation, regulations, and if applicable, contractual clauses for each business

4.2.3 Prevention of Misuse of Information Processing Facilities

Information processing facilities shall be used in accordance with the policies detailed in this document, the Acceptable Usage policy, and the Code of Business Conduct policy. Disciplinary action shall be taken for any violations of these policies

4.2.4 Compliance with Security Policies, Standards, and Technical Compliance

Department heads shall ensure that all security procedures within their area of responsibility are correctly carried out to achieve compliance with security policies and standards

4.2.5 Information Systems Audit Considerations

CNTXT shall conduct periodic audits by competent, independent parties to ensure compliance with information security policies, procedures, standards, and guidelines. Formal procedures shall be developed for planning and reporting audits, as well as addressing audit findings and implementing prompt and accurate remedial actions.

- Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed upon to minimize the risk of disruptions to business processes.
- Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for mode 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 within the organization.

End of Compliance 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