Organization of Information Security Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this document is to define an Information Security Management System (ISMS) governance framework within which the security organizational structure is identified, and information security roles, responsibilities, and authorities are assigned to ensure the segregation of duties. This policy is established to initiate and control the implementation of information security within the organization.

2. Scope

This document is applicable to all processes and operations within CNTXT that fall 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 responsibilities for information security at CNTXT will be clearly defined through job descriptions and task delegation. The Information Security Officer will approve the information security policy and standards. Responsibilities include identifying information assets, classifying them, implementing controls, and reviewing user access privileges. Segregation of duties and appropriate contact with authorities and special interest groups are emphasized. Information security will be integrated into project management, and precautions for mobile devices and teleworking shall be outlined.

4. Organization of Information Security

4.1 Information Security Roles and Responsibilities

- All information security responsibilities related to the protection of CNTXT's sensitive information, information systems, and information processing facilities shall be clearly defined through job descriptions, work allocation, and task delegation.
- The Information Security Officer shall approve the information security policy.
- The Information Security Officer shall approve the standards, procedures, templates, and guidelines.
- The defined information security responsibilities shall be formally allocated and accepted across the organization. These responsibilities shall include:
    - Identifying the information assets and the security processes associated with each asset.
    - Defining and documenting the asset ownership, level of responsibility, and authorization levels.
    - Classifying, labeling, and handling information assets in accordance with CNTXT Data Classification Policy.
    - Identifying and Implementing controls necessary to adequately protect assets.

- Reviewing and approving user access privileges in accordance with the Access Control Policy & Procedure.

4.2 Segregation of Duties

- Segregation of duties should be considered before assigning roles to carry out business activities to reduce opportunities for deliberate or accidental misuse of infrastructure elements or software. For example, the ability to initiate, authorize, execute, and verify requests should be split so that no one person completes the entire request.
- Where segregation of duties is not possible, appropriate compensatory controls such as activity monitoring, audit trails, and management supervision shall be developed to detect misuse of access rights.
- When primary personnel is unavailable due to illness, being on vacation, or due to leave of absence and another person with a different role fills in, appropriate segregation or compensatory controls shall be considered.

4.3 Contact with Authorities

Appropriate contacts shall be established with law enforcement authorities, regulatory bodies, third-party vendors, hardware vendors, software vendors, and office security providers.

4.4 Contact with Special Interest Groups

- The objective of this guideline is to ensure that CNTXT maintains appropriate contact with special interest groups and authorized information security forums to receive and distribute updates on new vulnerabilities, security threats, regulations, or risks pertaining to its business.
- The Information Security Officer at CNTXT will ensure that contacts with Special Interest Groups are maintained in the interest of CNTXT's security posture. The Information Security Officer shall consider maintaining contacts with the following types of special interest groups, but not limited to:
    - Special Security Forums: These forums enhance the security of communications and information infrastructure through proactive action and effective collaboration with other security bodies. These forums issue security guidelines and advisories and share information relating to the latest changes in information security. These forums help in reporting local problems.
    - Security Advisories: Security advisories provide objective, timely, and comprehensive information about security threats and vulnerabilities. An example could be certain security advisory websites.
    - Application Vendors/suppliers: Contacts with vendors/suppliers for applications used within the CNTXT environment should be maintained to ensure that the latest threats and vulnerabilities applicable to these applications are addressed.

    - Other institutions that can help in solving security issues.
- The Information Security Officer shall be associated with the above companies/institutions with the objective to:
    - Get updates on new vulnerabilities, security threats, and regulations pertaining to the telecom industry.
    - Improve knowledge and keep up-to-date with relevant security information.
    - Ensure that the understanding of the information security environment is current and complete.
    - Receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities.
    - Gain access to specialist information security advice.
    - Share and exchange information about new technologies, products, threats, or vulnerabilities.

4.5 Information Security in Project Management

- Information security shall be integrated into CNTXT' project management methods to ensure that information security risks are identified and addressed as part of projects.
- Information security implications shall be taken care of regularly in all projects.

4.6 Mobile Devices & Teleworking

4.6.1 Mobile Device Policy

- When traveling (in cars, hotels, conferences, meeting rooms, and public places), employees shall take reasonable precautions to protect their laptops as much as possible from damage, theft, and eavesdropping. If left unguarded, the laptop should be concealed as far as possible (e.g., locked in the trunk/boot of the car). Normally an unattended laptop should be in shutdown mode, and an unattended laptop should never be accessible without password protection.
- The loss of a laptop/mobile device must be reported immediately to the HR Team or the Project Manager.
- An employee may not make any alterations that circumvent the security mechanisms of CNTXT for their laptop. In addition to disciplinary measures, the employee may also be charged for the costs incurred by CNTXT if the laptop is damaged through unacceptable manipulation. Unacceptable manipulation includes, for example:
    - Autonomous set-up of unauthorized Internet connections.
    - Switching off the virus scanner, particularly with an open connection to the Internet.
    - Misusing privileges granted to enable certain business functions.
- Users are responsible for maintaining the confidentiality, integrity, and availability of the information on their mobile computing devices.

- The Information Security Officer shall ensure that all endpoints with access to the production infrastructure have antivirus software installed.

4.6.2 Teleworking

- Employees shall take all necessary precautions to secure information and equipment in their homes, prevent unauthorized access to any system or information and comply with the 'Acceptable Usage of Assets' policy.
- CNTXT's equipment must be protected against damage and unauthorized use. Employees need to designate a safe workspace at home that is free from hazards. Safeguards should be applied to protect records from unauthorized disclosure or damage. Wherever applicable, all records, papers, and correspondence should be safeguarded for their return to the office.
- Revocation of authority, access rights, and return of equipment should occur when teleworking activities cease or when the employee exits from CNTXT.

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 Organization of Information 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