Communications & Network Security Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

CNTXT shall take adequate precautions and design appropriate controls to prevent misuse of its information assets and information processing facilities. In this regard, CNTXT shall establish necessary communication and network security procedures, protect information in networks and support infrastructure, maintain the security of information being transferred, and detect any unauthorized information processing activities.

2. Scope

This document applies to all processes and operations within the scope of the Information Security Management System at CNTXT.

3. Policy Statement

CNTXT is committed to ensuring the highest level of service to its customers. Consequently, it is paramount to manage and control networks to protect them from threats and maintain the security of their systems and applications.

4. Communication & Network Security

4.1 Network Security Management

4.1.1 Network Controls

- Networks shall be adequately managed and controlled to be protected from threats and to maintain the security of the systems and applications using the network, including information in transit.
- Network-based intrusion prevention/detection system shall be deployed, wherever possible, to cover critical network segments within IT infrastructure.
- Infrastructure elements and software(s) exposed to un-trusted or semi-trusted networks/users (e.g., Internet-facing systems, distributors, call centers, Contract Partners, etc.) shall be adequately protected by firewalls, Intrusion Prevention Systems (IPSs), and limited connectivity and encryption.
- Any system deployed on the Internet must go through a thorough vulnerability check.
- All configurations must be done by trained and authorized personnel. Any changes to network configurations should follow the Operations Security Procedure.
- Vulnerability assessment of these infrastructure elements shall be carried out every year.
- All end-user systems connecting to the CNTXT infrastructure should have baseline security implemented.

4.1.2 Information Transfer Policies & Procedure

- Users shall be made aware, and information transfer guidelines shall be captured in the Data Classification Policy and Asset Management procedure, and users shall be made aware of these guidelines.
- Acceptable use standards shall be established to define guidelines for the appropriate use of communication facilities.
- Appropriate anti-malware controls shall be established to detect and prevent malware that could be transmitted through electronic communication channels.
- Employees shall treat all correspondence sent using CNTXT email systems as confidential.
- To prevent loss, modification, destruction, or misuse of information, CNTXT shall protect and control the exchange of critical business information assets and software with third parties and outside organizations.
- Where feasible, it is recommended to consider the implementation of appropriate web filtering mechanisms that will restrict user access to external networks and websites based on the organization's policies.

4.1.3 Electronic Messaging

- Information involved in electronic messaging (e.g., emails, instant messengers) shall be appropriately protected from unauthorized access, modification, or denial of service.
- Public email accounts shall not be used for conducting CNTXT operations unless authorized.
- Forwarding of CNTXT mailbox to public or non-CNTXT email accounts shall be done in accordance with the Data Classification policy.

4.1.4. Confidentiality or Non-Disclosure Agreements

- Confidentiality or non-disclosure agreements reflecting CNTXT needs for the protection of information shall be identified and maintained with all the third parties, and this will be based on the criticality of the information to be protected. These requirements shall be reviewed at least once in a year and at the time of any change in the business environment, legal requirements, and contractual obligations.
- Confidentiality and non-disclosure agreements shall comply with all applicable laws and regulations for the jurisdiction to which they apply.
- Both staff members and contract partners of CNTXT shall sign and comply with the non-disclosure agreement (NDA) that is established and maintained by the CNTXT's HR team, where applicable.

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 Communications & Network 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