Network Security Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

Network security shall help minimize information security risk to a great extent and protect the organization against the threat of unintended information disclosure. CNTXT networks (includes Cloud, VPC, and cloud services) must be protected from internal and external intrusion by designing network security at a level that is appropriate for the nature of data transmitted to protect all business data, related application systems, and operating systems software from unauthorized or illegitimate access. It is imperative to establish controls that protect CNTXT networks against information security threats.

The primary use of this document is to provide guidance for implementing Network Security controls.

2. Scope

This document is applicable to all processes and operations in CNTXT within the scope of the ISMS.

3. Network Security Management

3.1 Network Control

- The Engineering Team should have designated employee(s) for managing the CNTXT networks which include cloud environments, VPCs, and cloud services like Office 365 and Google Workspace.
- Where feasible, WAF should be configured to automatically provide protocol anomalies reports, traffic analysis, system malfunction signals, etc.
- Any changes to the network configurations should follow an appropriate change management process.
- Where feasible, logs of these tools/devices should be regularly monitored by the administrators or by using any third-party IDS/IPS tools.
- Any anomaly detected is raised as an information security incident through proactive monitoring, wherever applicable and implemented (examples include AWS Guard Duty or Microsoft Defender etc.).
- The Engineering Head should ensure that data passing through the network is encrypted using appropriate encryption techniques wherever feasible.

3.2 Security of Network Services

- The Engineering department should identify the security requirements for the network. These include requirements such as, but not limited to:
    - Encryption;
    - Intrusion detection and prevention system; and
    - Network monitoring.

- The Engineering team should ensure that all the identified network security requirements are implemented for the cloud infrastructure owned by CNTXT.
- If the network services are procured from a third-party service provider, these security requirements should be embedded in the network services agreement, signed with the network service provider.
- The Information Security officer along with the Engineering team is responsible to ensure a third-party independent network assessment is carried out annually to provide assurance to the management, stakeholders, and other parties involved, and to meet any regulatory requirements. This assessment can be a part of a VAPT exercise as well.
- Once the assessment has concluded, results should be documented and officially communicated to the Engineering team to remediate any security issues.
- After waiting for allowable time to recover and correct any security issues, the Engineering team should arrange to conduct another test to verify that communicated security issues were addressed and corrected.

3.3 Network Access Control

3.3.1 Use of Network Services

- The Engineering Team should restrict access to any production networks.
- The list of users having access to the production network must be maintained, preferably. Wherever, auto-generation of this list is not possible, it is recommended to manually maintain this.
- Information Security Officer along with Engineering Head should review the access to the production network on a quarterly basis.

3.3.2 Remote Diagnostic & Configuration Port Protection

All remote access to infrastructure should be configured in a manner such that diagnostic and configuration services are accessible through a dedicated in-band management network interface, over an encrypted application layer protocol such as SSL or SSH only.

3.3.3 Segregation of Networks

- Networks should be segregated into Virtual Private Cloud (VPC) subnets provided within cloud service platforms.
- The data flow between separate network domains should be controlled via secure gateways.
- Through a public subnet, the gateway allows respective employees to access either the production or development environment based on their respective roles.

- The Engineering Team is responsible for granting access to the production and development environment based on provided user roles and responsibilities.

3.3.4 Remote Devices

- All devices (Laptops) that access production infrastructure must run current versions of anti-virus software with regularly updated virus definitions.
- Users at public hotspots must be aware that, if such a remote device is not running a firewall, a malicious user can gain access to the remote device and install software or remove files from the remote device's hard drive.

4. Document Security Classification

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

5. 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.

6. 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.

7. Schedule

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

End of Network Security 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