Operation Security Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective
2. Scope
3. Policy Statement
4. Operations Security Policy
5. Document Security Classification
6. Non-Compliance
7. Responsibilities
8. Schedule
9. Version history

1. Objective

The objective of this policy is to provide guidelines to ensure the secure processing of CNTXT's production infrastructure and ensure there are no disruptions to the availability of CNTXT's services through adequate planning, operating procedures, back-up, change management, logging, and vulnerability management.

2. Scope

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

3. Policy Statement

CNTXT shall take adequate precautions and design appropriate controls to prevent misuse of its information assets and ensure that any operational activities at CNTXT do not affect the confidentiality, integrity, and availability of CNTXT's services. In this regard, CNTXT shall ensure to maintain the appropriate level of information security, minimize risks of system failures, protect the integrity of software and information, maintain the integrity and availability of information, protect information in networks and infrastructure, prevent unauthorized disclosure, manage technical vulnerabilities, maintain security of information and software exchanged and detect any unauthorized activities.

4. Operations Security Policy

4.1 Change Management

- Formal change management procedures shall be established to ensure controlled changes of all critical elements that affect information security which may include but are not limited to software, production infrastructure, network devices, configurations, and documented policies and procedures.
- It is recommended that the procedure should consider how to handle scheduled and emergency changes.
- All changes shall be recorded, approved, and tested before being implemented.
- It is essential to have all the changes, along with approvals, recorded in centralized systems like version control systems or ticketing tools.
- The requestor, reviewer/approver, and implementer's responsibilities for addressing the change shall not rest with the same user to ensure segregation of duties.
- Changes should be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, assess its impact on operations and security, and verify that only intended and approved changes were made.

- The production environment shall be separated from other environments to reduce the risks of unauthorized access or changes to the operating system.
- Modifications to vendor-supplied products should be discouraged. Vendors must be intimated if a change is warranted to obtain system patches/releases and ensure that security and functionality features are not impacted. The original software shall be retained, and changes shall be documented.

4.2 Capacity Management

- Critical parameters and their thresholds shall be monitored for all critical infrastructure elements and software(s) at periodic intervals to ensure required performance levels and availability.
- Capacity planning shall take into account current and projected trends in the organization's information-processing capabilities.
- System monitoring shall be enabled to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls like alerts or alarms shall be put in place to indicate problems in due time.

4.3 Configuration Management

- Configuring baselines for critical infrastructure and software should be established and documented where required. Such baselines include server hardening, end-point device hardening, firewall, and network device configurations. It is the decision of the organization whether such documentation is required or not.
- Any change to existing configurations of all production infrastructure, network devices, and firewall configurations must always follow the change management process and must be approved before such configuration changes are made.
- If the baselines are documented, any change must be approved and appropriately documented. It is recommended to follow the change management process for such a change.
- Clock synchronization configurations should be taken care of across all cloud infrastructure, cloud services, and endpoints. It is recommended to ensure they are synced depending on time zones to ensure that integrity and traceability of data are maintained.

4.4 Backups

- All original customer data on the infrastructure operated by CNTXT should be backed up.
- The frequency of such backups should be decided based on the risk considered to the organization and service level commitments made to customers and stakeholders.
- A backup restoration exercise must be performed to ensure that the backup data is readable and usable in case of any emergency or disaster.

- Backups must be stored at a redundant location outside the production environment itself. The number of such redundant locations should be decided based on perceived operational risks.
- In case CNTXT has any on-premise production servers and data, if required, appropriate procedures to take backups on physical media and a procedure to store it at offsite locations must be considered to minimize risks.
- Relevant documented processes/procedures shall be created and followed to meet the business requirements. The process/procedures shall define as follows:
    - Frequency for taking backup and testing of backup through a restoration process.
    - Data to be backed up.
    - Type of backup (incremental, differential, full).
    - The testing procedure for ensuring that the backup media can be relied upon in an emergency. Backup data shall be periodically restored, and the results be recorded. If the restoration test fails, the data owner should be notified regarding the same. Root cause analysis for such failure should be carried out.
    - Instructions to restore in case of an actual disaster.
    - The retention period for backup.

4.5 Logging and Monitoring

- Infrastructure elements and software used for CNTXT's operations should be configured, where feasible, to capture security-relevant logs (e.g., use of privileged accounts like root and administrator accounts, system failures, policy violations, unauthorized access attempts, logging of firewall traffic).
- Such monitoring and logging activities shall also consider information requirements for logging prescribed under legal and contractual requirements, if any. Evidence shall be collected, retained, and presented where legal actions are required following an information security incident or regulatory information provision.
- Logs shall be securely maintained for a minimum period stipulated as per applicable laws and regulations to provide support for investigations of incidents.
- Logging facilities and log information shall be protected against tampering and unauthorized access.

4.6 Control of Operational Software

CNTXT does not allow the installation of any other software on our production infrastructure.

4.7 Technical Vulnerability Management

- There shall be a documented procedure for technical vulnerability management.
- Timely information about technical vulnerabilities in infrastructure elements and software(s) being used shall be obtained from trusted sources.

- Where possible, tool-based vulnerability scans shall be carried out for all critical infrastructure elements and software(s).
- Once every year, it is recommended to have a vulnerability assessment performed by a 3rd party vendor.
- Timelines shall be defined for responding to identified/reported technical vulnerabilities.
- Information obtained regarding vulnerability shall be evaluated to assess risk to CNTXT's infrastructure. The evaluation shall take into consideration the following:
    - Vendor/tool reported criticality (e.g., high, medium, and low).
    - Likelihood of the vulnerability being exploited (e.g., the existence of a known exploit or other malicious code that uses the vulnerability as an attack vector).
- The identified risk shall be categorized as per the severity of the risk (e.g., High, Medium, and Low).
- If the vulnerability closure requires patch deployment, the patch must be tested in a test environment before deployment to the production environment.
- The system shall be checked to verify if the patch has not affected any of the existing functionality.
- For high-risk vulnerabilities, after applying the patch/solution, a check shall be performed to ensure that the vulnerability has been closed.

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 Operation 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