Asset Management Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this document is to describe a formal procedure to be followed for maintaining, handling, and protecting all the information assets of CNTXT.

2. Scope

This procedure applies to all the employees at CNTXT who use or have access to CNTXT's information assets and data.

3. Asset Management Procedure

3.1 Inventory of Assets

- At all times, the updated inventory of assets shall be maintained.
- A list of information assets like infrastructure, code repositories, software, and people assets are automatically maintained using cloud service providers, version control systems, identity providers, or HRMS applications (if applicable), respectively.
- For assets where inventory cannot be maintained automatically, it is the responsibility of the Information Security Officer to document the use of other software assets that have access to sensitive information.
- CNTXT allows employees to bring their own laptops or CNTXT issued laptops in some cases. For all such end-point devices, employees are responsible for reporting the device that they use to access CNTXT's data. The guidelines to maintain the security of endpoint devices shall be made available to all users through the Endpoint Security Policy.
- It is the responsibility of the People Operations Head to ensure that all employees have reported the status of devices used by them.
- The inventory of assets should also include the asset owner. Asset owners shall be responsible for maintaining and updating the inventory of the assets.
- The Information Security Officer or Infra Operations Person must verify the information asset inventory once it is created and at least on an annual basis thereafter.

3.2 Managing Infrastructure Assets

- Any new infrastructure asset acquired by CNTXT should automatically be tracked in the inventory that is maintained. In case it is not tracked automatically or in the event of a non-success, the Infra Operations Person or Information Security Officer must ensure the asset list is updated periodically.
- The Infra Operations Person is responsible for the classification of all infrastructure assets. The classification scheme is based on the type of data that the assets process and their criticality to services. The classification should be based on the Data Classification Policy.

- Based upon the classification of assets, there are security controls implemented to safeguard the integrity of the asset. These security controls are tracked along with the inventory of assets.
- The status of the security controls is automatically monitored through tools that integrate with cloud service providers/version control systems.
- If any of the security controls fail, an automatic alert is sent to the Infra Operations Person, who will be responsible for implementing the necessary changes promptly.
- If the controls are not implemented within the stipulated time, the security gaps are escalated automatically to the Information Security Officer, who will need to take necessary rectifying measures.

3.3 Managing End Point Assets

- CNTXT allows employees to “Bring your own device” for their company operations. The list of all the end-point devices is maintained.
- All employees need to report the devices that they use to access CNTXT’s data.
- If maintained manually, it is the responsibility of the Information Security Officer to ensure that periodic requests are sent at least once a quarter to all employees to report their device security status.
- It is the responsibility of users to follow the recommended steps below to ensure the security of endpoints:
    - CNTXT staff is responsible for installing critical firmware and software updates on the endpoints they use or where they’re the assigned owner.
    - CNTXT requires that all endpoints with access to critical data to use antivirus software to protect from malware.
    - CNTXT requires that all endpoints with access to critical data to turn on the hard disk encryption option of their respective operating systems (ex: FileVault on Mac).
    - As detailed in the access control policy, CNTXT staff members should use strong passwords to protect against unauthorized access to their system or any services they use. While it is not mandatory, it is recommended to use a password manager.
    - CNTXT requires that all endpoints with access to critical data to have auto-screen-lock on their systems within a reasonable amount of inactive period. While the screen lock will protect the device in most cases, it is recommended not to leave the computer unattended and unlocked.
    - Employees must immediately report lost, stolen, or damaged devices to the CNTXT management, which will then attempt to constrain access to production systems and customer data through the exposed device.
    - Employees must follow the removable media guidelines outlined in the Asset Management and Physical and Environmental Security policies.
    - Endpoints may be verified for compliance with this policy through various methods, including but not limited to periodic reviews, automated monitoring, and internal and external audits.

3.4 Review of Assets

The Infra Operations person and the Information Security Officer must review the list of Infrastructure assets and critical systems at least annually.

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 Asset Management 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