Asset Management Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this document is to provide a framework to ensure that CNTXT's information assets and data are protected and handled appropriately.

2. Scope

This policy shall be applicable to assets used across all processes and operations within the scope of the ISMS at CNTXT.

3. Policy Statement

The Asset Management Policy is established to ensure that all CNTXT assets are classified and appropriately protected and that information handling or exchange of information is in accordance with this classification. This shall prevent unauthorized disclosure, modification, removal, or destruction of assets and interruption to business activities.

4. Asset Management

4.1 Types of Assets

The following are examples of the types of assets that need to be considered as Information Assets:

- Infrastructure Assets: databases and data files, servers, and version control systems.
- Software Assets: application software, system software, development tools, and utility software.
- Physical Assets: computer equipment, communications equipment, removable media, and other equipment.
- Service Assets: computing and communications services, general utilities such as heating, lighting, power, air-conditioning, and third-party suppliers.
- People Assets: employees (full-time and part-time), customers, contractors.
- Paper Assets/E-Documentation: contracts, agreements, non-disclosure agreements, system documentation, user manuals, training material, operational or support procedures, business continuity plans, fallback procedures, audit trails, and archived information.

4.2 Responsibility of Assets

- All information and associated assets shall have an individual or department with management responsibility assigned to control the production, development, maintenance, use, and security of the information asset.

- Each asset shall have an Asset Owner and, if required, a nominated custodian who may be different from the Asset Owner.
- The owner shall be responsible for the following:
    - Ensuring that information and assets associated with information processing facilities are appropriately classified.
    - Defining and maintaining the security of the assets along with helping the Information Security Officer periodically review access restrictions and classifications, taking into account applicable access control policies.
- As information is important and pervasive throughout CNTXT, all users have an important role and a responsibility to protect the information entrusted to them. All users who may come into contact with sensitive information (non-public) are expected to familiarize themselves with the Asset Management Policy and the Asset Management Procedure.

4.3 Inventory of Assets

- At all times, the updated inventory of assets shall be maintained.
- There should be owners assigned to maintaining the asset inventory. The owners may be different based on the type of asset.
- At the minimum, the inventory of assets needs to include an asset ID, an asset classification, and an asset owner.

4.4 Acceptable Use of Assets

- Acceptable use of assets associated with information assets shall be clearly defined.
- All users (employees and contract partners) who use or interface with assets associated with CNTXT shall acknowledge their awareness of the acceptable use of assets.

4.5 Return of Assets

Upon termination, CNTXT employees and contract partners shall return / hand over all the organization's information assets under their purview.

5. Data Classification

- Information assets shall be classified based on their business value, legal requirements, sensitivity, and criticality to the organization.
- It is important to understand the type of data the information asset processes to ensure that assets are handled appropriately. Please refer to the Data Classification Policy for more details.

6. Management of Removable Media

Usage of removable media such as a USB or hard drives to transfer data shall be prohibited. Any such use shall be deemed as non-compliance with this policy.

7. Disposal of Media

- Disposal of media, both electronic and physical, is important to ensure that data is protected from exposure to unauthorized people.
- Media shall be disposed of securely, following the formal guidelines when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the Data Classification policy.
- Please refer to the Media Disposal policy for guidelines and details.

8. Document Security Classification

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

9. 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.

10. 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.

11. Schedule

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

End of Asset Management 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