IT Asset Management Policy

Doc. Control Number	Version
SNL-09	1.1

Document Reference

Item	Description
Title	IT Asset Management Policy
Department	Cybersecurity department
Version No	1.1
Status	Draft
Type	DOCX
Publish-Date	5 March 2024
Revision-Date	5 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/3/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/3/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/3/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	19 Aug 2021	Muhaned Ali	First Release
0.2	2 Aug 2022	Muhaned Ali	Policy update
0.3	26 April 2023	Muhaned Ali	Asset discovery has been added
1.0	7 July 2023	Muhaned Ali	The Policy has been revised and updated.
1.1	5 March 2024	Muhaned Ali	Policy has been reviewed and updated

Contents

1. Overview

This policy outlines the principles and guidelines for protecting information within the organization. It covers the classification of information, privacy considerations, information transmission and retention, and the implementation of security mechanisms. The policy aims to ensure the confidentiality, integrity, and availability of information assets, as well as compliance with relevant cybersecurity regulations and standards.

2. Purpose

The purpose of this policy is to set out the rules for how assets must be managed from an information security perspective.

3. Scope

This policy applies to any IT assets purchased by or on behalf of SNLC.

4. Asset Discovery

4.1 Asset Inventory

a) An inventory of information assets shall be established and maintained by the IT team.

b) The inventory shall include all relevant information about each asset, such as asset type, location, owner, classification, and any associated dependencies.

c) Regular asset discovery processes shall be conducted to identify and add new assets to the inventory.

d) Asset discovery methods may include network scanning, physical inspections, documentation reviews, and coordination with relevant departments.

4.2 Asset Classification and Ownership

a) Each information asset shall be classified based on its importance, sensitivity, and criticality to the company.

b) Asset ownership shall be clearly defined, assigning responsibility to appropriate individuals or departments.

c) Asset owners shall be accountable for the proper management, protection, and maintenance of their assigned assets.

4.3 Frequency of Asset Inventory Updates

a) The asset inventory shall be updated regularly to reflect any changes in the status, location, ownership, or classification of assets.

b) Assets must be reviewed once a month and upon significant change, and any updates must be documented.

c) The specific frequency for updating the asset inventory shall be determined based on the company's needs and risk assessment.

4.4 Documentation and Recordkeeping

a) All changes, updates, and modifications to the asset inventory shall be documented and recorded in a centralized repository.

b) The IT team shall maintain accurate and up-to-date records of the asset inventory and associated changes.

4.5 Asset discovery tool

a) The IT team utilizes the GLPI tool to discover and identify all information assets belonging to the company and update the asset inventory.

5. Asset Classification Protection

5.1 All information assets within SNLC shall be classified based on their sensitivity, criticality, and regulatory requirements.

5.2 Classification Levels and Criteria

All information within SNLC will be subject to security classification. The information classification scheme requires information assets to be protectively marked as one of three classifications (excluding public information which does not need to be marked). The way the information is handled, published, moved, and stored will be dependent on this scheme.

The classes of information are:

- Level 1: Internal Use Only
- Level 2: Restricted
- Level 3: Confidential

The decision regarding which classification an information asset should fall into will be based on the following main criteria:

- **Legal** requirements that must be complied with.
- **Value** to the organization.
- **Criticality** to the organization.
- **Sensitivity** to unauthorized disclosure or modification

All classified information must be clearly labelled with the classification that has been assigned, so that employees, contractors and third parties are aware of the level of protection that must be applied, in accordance with SNLC procedures.

5.3 Asset Labeling and Handling

a) All information assets shall be clearly labeled with their respective classification level using standardized labels and markings.

b) Employees and authorized personnel shall handle and process assets in accordance with their assigned classification level.

c) Asset owners shall ensure that access controls, encryption, and other protective measures are appropriately implemented based on the asset's classification.

5.4 Asset Transfer and Storage

a) When transferring assets internally or externally, appropriate protective measures shall be employed, such as secure transmission channels, encryption, or physical security measures, based on the asset's classification level.

b) Storage of assets shall follow secure practices, including access controls, encryption, physical security measures, and regular backups, as per the asset's classification.

5.5 Asset Return, Deletion, and Disposal

a) Assets in physical form (e.g., documents, removable media) shall be returned or disposed of securely when no longer required, following approved procedures and in compliance with organizational policies and legal requirements.

b) Electronic assets shall be securely deleted or disposed of following approved procedures, ensuring data cannot be easily recovered.

5.6 Privacy, Ownership, Protection, Transmission, and Retention

a) Privacy

Personally identifiable information (PII) or other sensitive information collected, stored, or processed by the company shall be protected in compliance with applicable privacy laws and regulations. Privacy policies and procedures shall be established and communicated to all personnel.

b) Ownership

Information assets shall be clearly assigned ownership responsibilities. Owners shall ensure proper protection, handling, and use of the information.

c) Protection

Security controls shall be implemented to safeguard information assets against unauthorized access, modification, or destruction. Access controls, encryption, authentication, and other security mechanisms shall be employed as appropriate.

d) Transmission

Information transmitted over networks or other communication channels shall be encrypted and protected to prevent interception or tampering.

e) Retention

A retention period for information shall be determined based on organizational requirements and relevant legislation. Critical information shall be retained only for the necessary duration and disposed of securely when no longer needed.

5.7 Information Classification Process

a) Categorization

Information assets shall be categorized based on the classification criteria specified in the requirements document. This process shall ensure consistent and accurate classification of information across the company.

b) Handling of Critical Information

Critical information, based on factors such as business value, legal obligations, technical requirements, and national and cross-border regulations, shall be handled with extra care. Additional security measures, access controls, and monitoring mechanisms shall be implemented to protect critical information from unauthorized disclosure, alteration, or loss.

5.8 Security Mechanisms

a) Cryptography and Data Loss Prevention

- Cryptography

  Encryption techniques shall be used to protect information in transit, at rest, and in use. Cryptographic algorithms and key management practices shall comply with established requirements for cryptography.

- Data Loss Prevention (DLP)

  Data loss prevention techniques shall be employed to prevent unauthorized data disclosure or exfiltration. This includes monitoring, detection, and prevention measures to mitigate the risk of data breaches or leaks.

5.9 Information Transmission and Usage in Test and Development Environments

Information from production environments shall not be transmitted to other environments without appropriate safeguards. Critical systems data shall not be used in test and development environments unless necessary and strictly controlled to prevent unauthorized access, exposure, or misuse.

5.10 Retention and Disposal

Information retention periods shall be defined based on organizational requirements and relevant legislation. Critical information shall only be retained for the necessary duration and disposed of securely using approved methods, ensuring that data is irrecoverable and does not pose a risk to the company.

5.11 Continuous Measurement, Review, and Optimization

The requirements for information protection, including classification, security mechanisms, and compliance with regulations, shall be continuously measured, reviewed, and optimized. Regular assessments, audits, and evaluations shall be conducted to ensure the effectiveness of the process and identify areas for improvement. Any identified vulnerabilities, risks, or non-compliance issues shall be promptly addressed and remediated.

6. Policy Review

6.1 This policy shall be reviewed at least annually or as required by changes in regulations, organizational needs, or industry best practices. Amendments to the policy shall be approved by the appropriate authority and communicated to all relevant stakeholders.

7. Implementation And Compliance

7.1 Compliance

a) Non-compliance with this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, and legal consequences, as appropriate.

7.2 Implementation

a) All Departmental Managers are responsible for the implementation of this policy.

b) All Departments in IT and Information Security shall be responsible for compliance with this policy.