



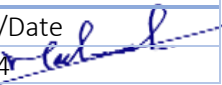
Information Protection Policy

Doc. Control Number	Version
SNL-73	0.2



Document Reference

Item	Description
Title	Malware Handling Policy
Department	Cybersecurity Department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	31 March 2024
Revision-Date	31 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	31/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	1/4/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	1/4/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	31 March 2023	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Overview	4
2. Scope	4
3. Policy	4
4. Policy Compliance	5

1. Overview

At Saudi Net Link Company, we recognize the critical importance of protecting sensitive information to maintain the trust of our customers, partners, and stakeholders. The Information Protection Policy outlines our commitment to safeguarding data assets and ensuring compliance with relevant regulations and industry standards. This policy establishes guidelines for the classification, handling, transmission, and retention of information to mitigate risks associated with data breaches, unauthorized access, and misuse. By adhering to this policy, we aim to uphold confidentiality, integrity, and availability of information across all business operations.

2. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to Saudi Net link company's information assets.

3. Policy

3.1 Asset Classification

- a) **Classification Levels:** Information shall be classified into three levels: **Restricted**, **Confidential**, and **Public**, based on sensitivity and impact on the company.
- b) **Criteria for Classification:** The classification shall be determined by factors such as sensitivity, criticality, legal/regulatory requirements, and business impact.

3.2 POPTR

- a) **Privacy:** Personally identifiable information (PII) and sensitive data shall be handled with strict privacy controls to ensure compliance with applicable privacy laws and regulations.
- b) **Ownership:** Information ownership shall be acknowledged, and appropriate controls shall be implemented to protect the rights of stakeholders.
- c) **Protection:** Security mechanisms, including encryption, access controls, and data loss prevention techniques, shall be employed to safeguard information in transit, at rest, and in use.
- d) **Transmission:** Information shall not be transmitted from production environments to other environments without proper authorization and encryption mechanisms.
- e) **Retention:** A retention period shall be determined for each category of information based on organizational requirements and relevant legislation. Retention of critical information shall be restricted to necessary requirements only.

3.3 Information Classification Process

- a) **Categorization:** Information shall be categorized based on predefined criteria, considering business value, legal obligations, technical requirements, and national/cross-border considerations.
- b) **Handling of Critical Information:** Critical information shall be managed according to defined criteria, considering its significance to the company.

3.4 Security Mechanisms

- a) **Encryption:** Strong encryption mechanisms shall be utilized to protect information in transit, at rest, and in use, in compliance with cryptography requirements.
- b) **Data Loss Prevention (DLP):** DLP techniques shall be implemented to prevent unauthorized disclosure or leakage of sensitive information.

3.5 Prevention of Information Transmission and Usage in Test/Development Environments

- a) Information transmission from production environments to other environments shall be tightly controlled and authorized.

- b) Usage of critical systems data in test and development environments shall be restricted and subject to stringent controls.

3.6 Retention Period Determination

- a) Retention periods for information shall be determined in accordance with organizational requirements and relevant legislations.
- b) Retention of critical information shall be limited to the necessary requirements, with regular reviews and updates to ensure compliance.

4. Policy Compliance

The Infosec team will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrust, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

4.1 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

4.2 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

