Configuration Management and Hardening

Doc. Control Number	Version
SNL-22	1.0

Document Reference

Item	Description
Title	Configuration Management and Hardening
Department	Cybersecurity department
Version No	1.0
Status	Draft
Type	DOCX
Publish-Date	31 May 2023
Revision-Date	31 May 2024

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/31/2023

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/31/2023

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/31/2023

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	19 Jan 22	Muhaned Ali	First Release
0.2	25 July 22	Muhaned Ali	Policy Updated
0.3	31 May 2023	Muhaned Ali	The policy has been reviewed and updated.
1.0	31 March 2024	Muhaned Ali	The policy has been reviewed

Contents

1. Purpose

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards related to protecting, fortifying, and configuring SNLC's information and technical assets and applications to resist cyber-attacks by focusing on the primary objectives of protection: confidentiality, integrity, and availability of information.

2. Scope

This policy covers all informational, technical, and application assets of SNLC, and applies to all employees of SNLC.

3. Policy

a) All information and technology assets used within SNLC, as well as approved applications and software, must be identified and ensured that technical security standards are in place for them.

b) All information and technology assets used within SNLC, as well as approved applications and software, must be identified and ensured that technical security standards are in place for them.

c) All asset configurations should be compliant with the SNLC baseline configuration.

d) Monitor and verify configuration settings against the baseline settings.

e) The settings of SNLC's computers, systems, applications, network devices, and security devices must be fortified and adjusted in accordance with the approved security technical standards to resist cyber-attacks.

f) One of the following methods should be used to develop technical security standards:

- Supplier Security Configuration Guidance in accordance with SNLC regulatory policies and procedures, relevant legislative and regulatory requirements, and international best practices.
- Configuration and hardening guide from reliable, industry-standard compliant sources such as the Center for Internet Security (CIS), Institute for Security, Network and Systems Administration (SANS), National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA), and Security Technical Implementation Guide (STIG), and others.
- Develop SNLC technical security standards appropriate to the nature of the business.

g) The controls for security technical standards shall cover, at a minimum, the following:

- Disable or change factory and default accounts.
- Prevent unwanted software installation.
- Disable unused network ports.
- Disable unused services.
- Restrict the use of external storage and media.
- Change default settings that may be exploited in cyber-attacks.

h) The settings and hardening must be reviewed and ensured that they are applied in the following cases:

- Review the settings and hardening of information and technical assets and applications periodically and ensure that they are applied in accordance with the approved technical security standards.
- Review the settings and hardening before launching and launching projects and changes related to information and technology assets.
- Review settings and hardening before launching and launching applications.
- Periodically review the settings and hardening of industrial control systems and ensure their application is in accordance with the approved technical security standards.

i) An image of the settings and hardening of the information and technology assets of SNLC must be approved in accordance with security technical standards and kept in a safe place.
j) An approved image must be used to install or update information and technology assets.
k) The necessary technologies to manage settings and hardening must be provided centrally, and to ensure that the settings and immunization can be automatically applied or updated for all information and technical assets at specific and planned time dates.
l) A Performance Measurement Indicator (KPI) should be used to ensure the continuous development of the management of settings and hardening.
m) The cybersecurity requirements relating to the preparation and hardening of SNLC's information and technology assets, and applications should be reviewed annually, or in the event of changes in relevant legislative or regulatory requirements or standards.

4. Roles and Responsibilities

4.1 The sponsor and owner of the policy document: Head of Cyber Security Department.
4.2 Policy reviews and update: Cyber Security Department.
4.3 Policy implementation: IT Department

5. Policy Compliance

5.1 Compliance Measurement

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

5.2 Exceptions

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

5.3 Non-Compliance

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