Compliance Policy

Doc. Control Number	Version
SNL-04	0.3

Document Reference

Item	Description
Title	Compliance Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	4 March 2024
Revision-Date	4 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	4/3/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	4/3/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	4/3/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	13 Jan	Muhaned Ali	First Release
0.2	31 May 2023	Muahned Ali	The policy has been updated
0.3	4 March, 2024	Muahned Ali	The policy has been updated and reviewed.

Contents

1. Purpose

The purpose of this policy is to provide cyber security requirements based on best practices and standards in order ensure that the SNLC cyber security program complies with applicable legislative and regulations.

This policy aims to comply with the requirements of cybersecurity and the relevant legislative and regulatory requirements issued by the **CST**, **Aramco**, and **ISO 27001**.

2. Scope

This policy applies to all SNLC systems and procedures, as well as all SNLC employees.

3. Policy

3.1 The list of cybersecurity legislation and regulations, as well as associated requirements, must be recognized, documented, and updated at least annually or as per standard requirements.

3.2 The necessary technologies must be provided; To verify compliance with the requirements of legislative and regulatory authorities related to cybersecurity.

3.3 Technical reviews must be performed by competent people, and audit results must be documented and maintained.

3.4 Cyber security policies and procedures should be reviewed at least annually to guarantee compliance with relevant legislative and regulatory requirements.

3.5 Ensure that cyber security policies and procedures are applied on a regular basis.

3.6 Ensure compliance with appropriate legislation and regulatory requirements, Using appropriate tools such as:

- Cybersecurity Risk Assessment.
- Vulnerabilities Management.
- Penetration Test.
- Review of cyber security standards.
- User surveys.
- Interviews with stakeholders.
- Review the authorization access on the system and the network.
- Reviewing cyber security incidents and records.

3.7 The necessary corrective actions must be identified and implemented; To correct gaps in all compliance requirements by stakeholders.

4. Compliance Review

4.1 Annual audits of information systems should be performed to ensure compliance with the SNLC's information security policies and standards.

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.