Cyber Security Strategy 2023-2024

Reducing Risks, Enhancing Resilience

Doc. Control Number	Version
SNL-01	0.3

Document Reference

Item	Description
Title	Cyber Security Strategy
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	3/4/2024

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

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

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	12 Jan 2022	Muhaned Ali	First Release
0.2	17 May 2023	Muhaned Ali	Policy has been reviewed
0.3	4 March 2024	Muhaned Ali	Policy has been reviewed and updated

Contents

1. Massage from the V.P

It is critical that we safeguard our data, services, networks, programs, and other information against cyber dangers such as unauthorized or unintentional access, destruction, or change.

In collaboration with Aramco, CITC, and the NCA, Saudi Net Link will build a cyber security framework, support the Cybersecurity Department objectives, and monitor it on a regular basis.

Abdullah Al Shuhail________________________

2. Overview

SNLC wants to build, maintain, and improve its cybersecurity skills, as well as defend itself from internal and external cyber risks, and SNLC has prepared this cybersecurity strategy to fight threats, decrease cyber risks, and support an SNLC business strategy.

3. Purpose

The purpose of this policy is to provide recommendations related to cybersecurity work in SNLC in a way that is consistent with the nature of the work, to enable business initiatives, to provide a clear and unified vision, and to disseminate it among all departments and sections of SNLC, as well as its affiliates and companies.

4. Scope

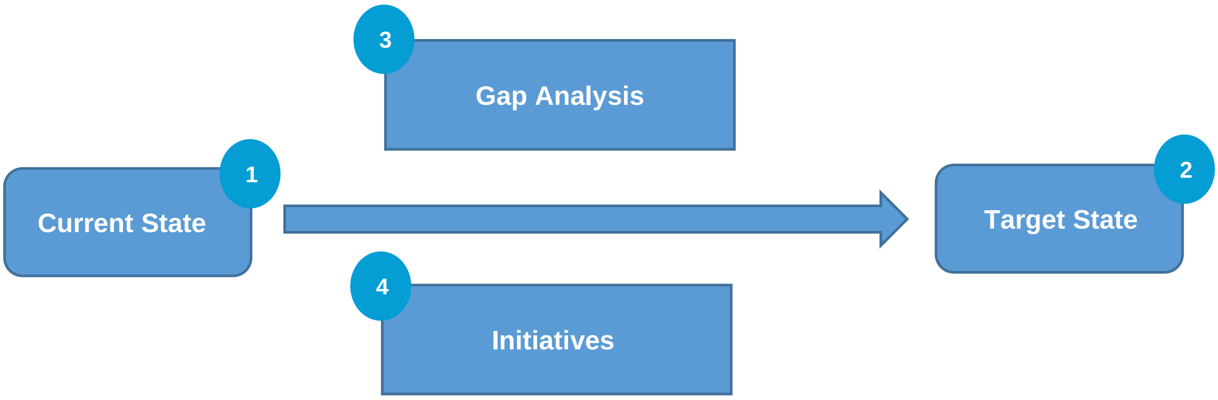
This policy applies to all SNLC's work. In turn, SNLC and its subsidiaries and agencies will be eager to put it into action.

5. Cybersecurity Vision

The cybersecurity vision provides a brief description of the position that SNLC aspires to achieve in terms of its cybersecurity situation, describes the future targeted position of cybersecurity in SNLC, and enables SNLC to gain access to a secure and reliable cyberspace in which to grow and prosper.

6. Inputs Into the Strategy

The Kingdom of Saudi Arabia's vision and orientations in the realm of cybersecurity are among the fundamental inputs in the formulation of SNLC's cybersecurity strategy. To match the objectives of its cybersecurity strategy with the objectives of the National plan, it is critical to understand the function of SNLC and its contribution to the national cybersecurity strategy.



7. Current State Cybersecurity

The activities below present examples of the inputs that make up the cybersecurity strategy for SNLC in accordance with the national cybersecurity strategy, and CITC. The objective of these activities is to define the target status of cybersecurity compared to the current situation:

1- Assess the level of compliance with regulatory and legislative requirements.
2- Cybersecurity Risk Assessment.
3- Cybersecurity Maturity Assessment.

8. Cybersecurity Objectives

The cybersecurity objectives have been defined in accordance with the cybersecurity vision and the results of the activities that are clarified in the Cybersecurity Current Status section, which are as follows:

1- Enhance cybersecurity domain.

2- Deploy additional tools for security management.

3- Maintain compliance with cybersecurity standards (CST, ISO 27001, ARAMCO CCC+, NCA).

9. Gap Analysis

Based on the results of the assessment of the level of compliance with the implementation of basic cybersecurity controls, cybersecurity risk assessment, business impact analysis, and cybersecurity maturity assessment, a SWOT analysis is conducted for SNLC to analyze the gaps between the current situation and the cybersecurity target situation in SNLC, and this analysis shows the strengths and weaknesses of SNLC, the opportunities that SNLC can exploit and the threats it faces.

10. Cybersecurity Initiatives

1- Cybersecurity initiatives include all projects and programs required to implement the objectives of the cybersecurity strategy. These initiatives are formed based on the cybersecurity vision and objectives:

- **Governance, Compliance, and Risk Management:** The initiative includes projects and programs in governance, risk, and commitment to enhance cyber security in SNLC and build strategic plans in cybersecurity.
- **Prevent and detect cyber threats:** The initiative includes projects and programs that help SNLC detect and prevent internal and external threats.
- **Cyber Security Architecture:** The initiative includes projects and programs that help SNL increase its cybersecurity maturity level and protect SNL from cyber risks.
- **Building the capacity of the workforce in the field of cybersecurity:** This initiative includes projects and programs aimed at raising cybersecurity awareness and enhancing SNL with skills and qualifications in the field of cybersecurity.

11. Cybersecurity Roadmap

1- Defining an action plan to achieve the objectives of the cybersecurity strategy.

2- The strategy provides the basic elements of the action plan consisting of cybersecurity initiatives that, in turn, achieve the cybersecurity objectives if implemented (the objectives are detailed in the cybersecurity objectives section).

3- The strategy's action plan includes items related to monitoring and performance indicators to determine the level of success, which enables comments to be submitted to the Cyber Security Supervisory Committee. This allows for amendments to the plan and ensures that cybersecurity initiatives are implemented correctly to achieve the goals.

4- The cybersecurity roadmap shows the way to distribute the initiatives to be implemented over the next three years, as priority is given to cybersecurity initiatives based on the results of risk analysis and business impact analysis (BIA) described in the risk assessment and business impact analysis section, and the roadmap gives priority to dealing with high risks, in addition to dealing with sensitive systems.

12. Cybersecurity Budget

The purpose of the cybersecurity budget is to determine the budget needed to implement the cybersecurity action plan and initiatives and to obtain the necessary funds to be allocated by the Department of Finance.

- Budget characteristics

  1- SNLC's Information security department is responsible for preparing the budget for cyber security as the best way to ensure the provision of techniques and tools related to cyber security, and it is responsible for providing a summary of expenditures related to the cyber security budget to whom it is provided.

2- A cybersecurity budget has been allocated to cover all costs of a cybersecurity action plan, so it must be accurate, logical, and comprehensive of the amounts expected to be disbursed.
3- The cyber security budget must be compatible with relevant policies, legislative and regulatory requirements, orders, and decisions.
4- The cyber security budget is determined based on the annual budget cycle of SNLC.
5- The cyber security budget is subject to a periodic review in accordance with the policies and procedures approved in SNLC.

- Budget Components

The cyber security budget includes the following components:

1- Operating budget for the department concerned with cyber security, which includes the following:
    - Cost of Cyber Security Staff
    - Cost of consulting services
    - Cost of technical services
    - Other costs
2- budget for cyber security initiatives, includes the following:
    - One-time costs of establishing a cybersecurity department and related processes to implement the cybersecurity strategy.
    - Recurring costs covering cybersecurity measures (e.g., cybersecurity management, monitoring, reporting, compliance, etc.).
    - The cost of specialized skills development programs and training needed for cybersecurity personnel, such as training courses and conferences.
    - The cost of outsourcing services.
3- Cyber Security Budget Calculation
    1- The cybersecurity budget that SNLC has allocated for the cybersecurity strategy that will run for the next three years is: (1,350,000) Saudi Riyals.

13. Roles and Responsibilities

13.1 The sponsor and owner of the document: Head of Cyber Security Department.
13.2 Document reviews and update: Cyber Security Department.
13.3 Document implementation: Cyber Security Department.