Cyber Security Organizational Structure

Doc. Control Number	Version
SNL-03	0.3

Document Reference

Item	Description
Title	Cyber Security Organizational Structure
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	18 July 2022	Muhaned Ali	First Release
0.2	14 May 2023	Muhaned Ali	Rules and responsibility have been modified
0.3	4 March 4, 2024	Muhaned Ali	Policy has been reviewed and updated

Contents

1. Purpose

The Cyber Security Department, which is independent of the Information Technology Department, was established in 2019 in accordance with relevant legislative and regulatory requirements.

The cybersecurity organizational structure has been developed based on best practices and standards to provide the necessary support to the cybersecurity department to enable it to carry out the tasks assigned to it as required. The Cyber Security Department is one of the main pillars of SNLC and is concerned with protecting information and technology assets from cyber risks.

2. Guidelines

1- Ensure that the Cyber Security Department is independent of the Information Technology Department.

2- Ensure that the cybersecurity department is linked to the head of the organization or his designer in SNLC so that he can influence key decisions related to cybersecurity in SNLC.

3- Ensure that the cybersecurity department's link is different from the information technology department's link.

4- Oversee the implementation of the Action Plan by the cybersecurity committee by monitoring, dealing with conflicts, and enforcing necessary measures for improvement.

5- Avoiding conflict of interest. Examples of conflict of interest include:
- Managing the viability of technical and information systems (or operational systems) and managing their operations at the same time.
- Applying cyber security requirements and ensuring compliance with them at the same time.
- The interests of the cyber security monitoring team conflict with the cyber security operations operating team.
- The security testing team has a conflict of interest with the application development team.

6- Ensure that the following roles are present as a minimum in the cybersecurity architecture:
- Cyber Security Governance.
- Cyber security compliance management.
- Cyber security risk management.
- Managing a cyber security strategy.
- Cyber security resilience.
- Cyber security awareness and training.
- Cyber security operations (cyber security monitoring and incident response).
- Data and information protection.

7- The following roles may be added to the cybersecurity architecture:
- Cyber security architecture.
- Data and information privacy.
- Manage login identities and permissions.
- Managing the cybersecurity infrastructure.
- Physical security.

3. Cyber Security Governance

1- Elements of an SNLC Organizational Structure

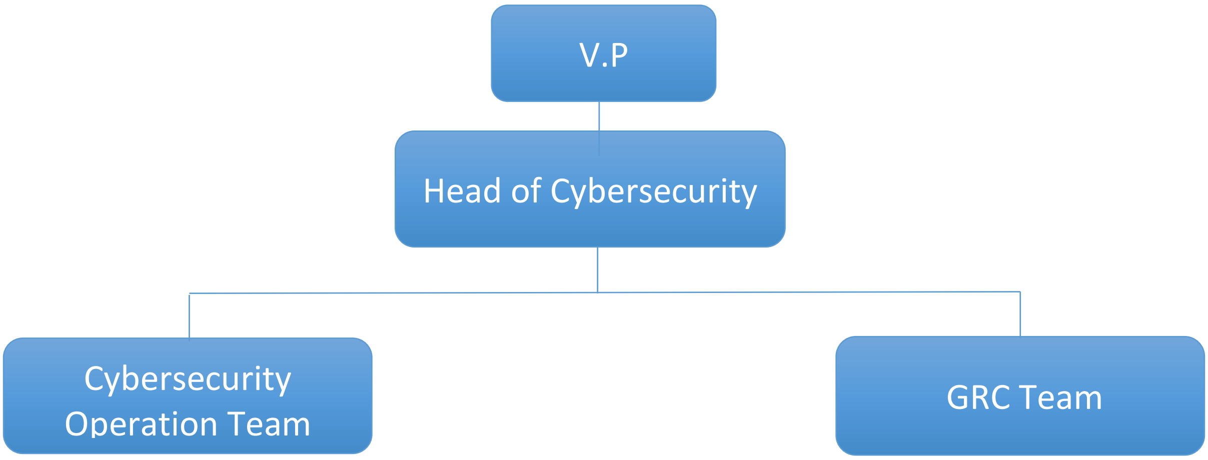
#	Element	Description
1	Business Owner	The authority holder (or his representative) is the highest authority in the entity, and it may be the board of directors.
2	Cyber Security Steering Committee	The Cyber Security Steering Committee is a high-level governance board, whose primary responsibility is to ensure compliance, support, and follow-up of the implementation of cybersecurity programs and legislation within SNLC.

3	Cyber Security Department	The Cyber Security Department is concerned with protecting networks, information technology systems, operational technology systems, their hardware and software components, the services they provide, and the data they contain from any penetration, disruption, modification, entry, use, or illegal exploitation. The concept of cyber security includes information security, cyber security, digital security, and so on.
4	Information Technology Department	The Information Technology Department is concerned with operating the information technology infrastructure and networks, developing software and technical services, and other business.
6	HR	The Human Resources Department is concerned with personnel matters within SNLC.
7	Legal Affairs	The Legal Department is the department concerned with drafting contracts and agreements and maintaining SNLC's legal rights.
8	Procurements	The Procurements Department is the department concerned with supplier contracting and procurement as well as third-party contracts in SNLC
9	Financial Affairs	The Finance Department is responsible for preparing the SNLC's overall budget.

2- Cyber Security Architecture

For the Department of Cyber Security to perform its work in the required manner and with high efficiency, the tasks and roles in the Department of Cyber Security were distributed based on the operational functions of each role, considering the principle of segregation of duties and conflict of interest and they were distributed as follows.

4. Organizational Structure of Cyber Security Department



Head of Cybersecurity		
#	**Roles**	**Responsibilities**
1	Cybersecurity Strategic Planning and Policy	Ensuring that the cybersecurity action plans, objectives, initiatives, and projects of the cybersecurity department contribute to achieving compliance with the relevant legislative and regulatory requirements.
2	Cybersecurity Risk Management	Ensure that cybersecurity risks are systematically managed to protect SNLC's information and technology assets, in accordance with SNLC's regulatory policies and procedures and relevant legislative and regulatory requirements.
3	Cybersecurity Compliance Management	Ensuring the implementation of cyber security requirements and compliance with relevant regulations and legislation.
GRC Team		
1	Cybersecurity Awareness and Training	Ensure that SNLC personnel have the necessary security awareness and are aware of their cybersecurity responsibilities. Ensure that SNLC personnel are equipped with the skills, qualifications, and training courses required in the field of cybersecurity to protect SNLC's information and technical assets and fulfill their responsibilities towards cybersecurity.
2	Cybersecurity Resilience	Ensuring that cybersecurity resilience requirements are met in SNLC's business continuity management. and ensuring that the effects of disruptions to critical electronic services in SNLC, its information processing systems, and devices due to disasters arising from cyber events are addressed and minimized.
3	Data and Information Protection	Ensure the protection of confidentiality, integrity, and availability of SNLC data and information, in accordance with SNLC's approved organizational policies and procedures, and relevant legislative and regulatory requirements.
4	Third-Party and Cloud Computing Cybersecurity	Ensure that information and technical assets are protected from cyber risks related to third parties and ensure that cybersecurity requirements for cloud computing and hosting are implemented in accordance with the regulatory policies and procedures approved in SNLC, and the relevant legislative and regulatory requirements.
Cyber Security Operations Team		
1	Vulnerability Management and Penetration Testing	Evaluate and test the effectiveness of SNLC's cyber security enhancement capabilities and examine and discover technical vulnerabilities by simulating actual cyber-attack techniques and methods. And discover unknown security vulnerabilities that may lead to a cyber intrusion.
2	Cybersecurity Incident and Threat Management	Ensure the timely identification, detection, management, and effective handling of cybersecurity events and threats to prevent or reduce their negative impacts on SNLC's business.
3	Cybersecurity Monitoring	Ensure the collection, analysis, and monitoring of cyber security events to detect cyber-attacks early with the aim of preventing or minimizing their negative impacts on SNLC business.

5. 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: Cyber Security Department and HR Department.