




Cybersecurity Awareness Policy

Doc. Control Number	Version
SNL-05	0.3

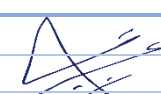


Document Reference

Item	Description
Title	Cybersecurity Awareness Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	5 March 2024
Revision-Date	5 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	13 Jan 2022	Muhaned Ali	First Release
0.2	5 July 2023	Muhaned Ali	The policy has been reviewed
0.3	5 March 2024	Muhaned Ali	The policy has been reviewed and updated



Contents

1. Overview	4
2. Scope.....	4
3. Policy Statement	4
4. Objectives	4
5. Responsibilities	4
6. Program Components	4
7. Compliance	7
8. Policy Review	7

1. Overview

The Cybersecurity Awareness Policy of SNLC aims to create a culture of cybersecurity vigilance among all employees, contractors, vendors, and stakeholders. This policy outlines the organization's commitment to cybersecurity awareness and the responsibilities of all individuals associated with the organization in safeguarding its digital assets and sensitive information.

2. Scope

This policy applies to all SNLC employees, third parties, and consumers.

3. Policy Statement

SNLC recognizes that cybersecurity is a shared responsibility. All individuals associated with the SNLC must be aware of potential cybersecurity threats, adhere to best practices, and actively contribute to the protection of digital assets and sensitive information.

4. Objectives

The objectives of this policy are as follows:

- a) Promote Cybersecurity Awareness: To promote awareness of cybersecurity threats, risks, and best practices among employees, contractors, vendors, and stakeholders.
- b) Prevent Cybersecurity Incidents: To reduce the risk of cybersecurity incidents, data breaches, and security breaches through proactive awareness and vigilance.
- c) Compliance: To ensure compliance with industry regulations, standards, and SNLC's cybersecurity policies and guidelines.

5. Responsibilities

5.1 Management and Leadership

- a) Senior management shall champion cybersecurity awareness and allocate necessary resources to support awareness initiatives.
- b) Management shall lead by example by following cybersecurity best practices and encouraging their teams to do the same.

5.2 Information Security Team

- a) The Information Security Team shall develop and implement cybersecurity awareness programs, including training, communication, and incident response.

5.3 Human Resources

- a) Coordination of all training and awareness sessions.
- b) Maintaining training records
- c) Facilitating new employee training and awareness workshops

5.4 Employees, Contractors, Vendors, and Stakeholders

- a) All individuals associated with the SNLC shall actively participate in cybersecurity awareness initiatives and adhere to cybersecurity policies and guidelines.
- b) They are responsible for promptly reporting suspected security incidents to the Information Security Team.

6. Program Components

SNLC shall establish and maintain a comprehensive cybersecurity awareness program, which includes but is not limited to:

6.1 Training and Education

- a) Regular cybersecurity training sessions for all employees, with a focus on:
 - Internet and social media security
 - Phishing, Password security, and incident reporting.
 - Social Engineering
 - Cybersecurity Acceptable Use.
 - Data Security

6.2 Policies and Guidelines

- a) Providing access to and ensuring understanding of SNLC's cybersecurity policies and guidelines.

6.3 Security Updates and Alerts

- a) Communicating timely security updates, patches, and alerts to all employees and stakeholders.

6.4 Simulated Phishing Exercises

- a) Conducting periodic simulated phishing exercises to assess and improve employees' ability to recognize phishing attempts.

6.5 Reporting and Incident Response

- a) Clearly defined procedures for reporting suspected security incidents.

6.6 Awareness Campaigns

- a) Periodic cybersecurity awareness campaigns to reinforce key messages and engage individuals actively in cybersecurity practices.

6.7 Plan Details

- a) Training Plan

To ensure that staff of SNLC is equipped with the skills and required knowledge to protect SNLC information assets and to fulfil their information security responsibilities, specialist or security related skills training should be provided to staff in the SNLC's relevant functional area categories in line with their job descriptions.

The following table summarizes the training that must be carried out:

Role	Method	Q1 2024	Q2 2024	Q3 2024	Q4 2024
Operations Manager	Technical Training	ISO 27001- Foundation			
Engineering Manager	Technical Training		ISO 27001- Foundation		
GRC Team	Technical Training	ISO 27001 – Lead implementer	CISM		CRISC
Human Resource Manager	Induction Training	HR role in information security		What is required from HR, how they will perform in line with policies & why these requirements should be implemented	
IT Department	Induction Training	What is required from procurement, how they will perform in line with policies, and why these requirements should be implemented		Security+	
Network Engineer	Technical Training	CCNA		CCNP	
Network Security Engineer	Technical Training	NSE4	NSE5		NSE6
NOC	Technical Training	GVF 10,20	CCNA		GVF 21
Technician	Technical Training	GVF 10	GVF 20		CCNA
G.W Team	Technical Training	iDirect system		ITIL	

System Analysis	Technical Training	Python		PBI	
Sales Team	Technical Training	Customer service	Presales Course		ITIL

b) Awareness Plan

For personal to understand the importance of information security management and their own contribution to information security, accept policies and plans, and understand the consequences of breaching the information security rules, the following awareness plan is scheduled:

Target Audience	Channel	Awareness Title	Awareness Purpose	J a n	F e b	M a r	A p r	M a y	J u n	J u l	A u g	S e p	O c t	N o v	D e c
New Joining	Acknowledgements	Acceptable Use of Technology	Outlines the acceptable uses of information and related assets	Through-out the years, upon contractual arrangements with newly joining staff members.											
	Acknowledgements	Job Roles and Responsibilities	The employees' roles and responsibilities regarding information security												
	Acknowledgements	Disciplinary process	What is the disciplinary process for police violation												
	Induction Training	Information Security Training	What is required from the employees, how they will perform in line with policy, and why these requirements should be implemented												
Employees	Acknowledgements	Acceptable Use of Technology	Outlines the acceptable uses of information and related assets.	Through-out the year, employees are going to be grouped and have awareness session.											
	Acknowledgements	Job Roles and Responsibilities	The employees' roles and responsibilities regarding information security												
	Acknowledgements	Disciplinary process	What is the disciplinary process for police violation												
	Induction Training	Information Security Training	What is required from the employees, how they will perform in line with policy, and why these requirements should be implemented												

7. Compliance

Failure to comply with this Cybersecurity Awareness Policy may result in disciplinary actions, as outlined in the SNLC's disciplinary policy.

8. Policy Review

This policy shall be reviewed annually or more frequently, if necessary, to ensure its effectiveness in addressing emerging cyber threats and promoting a culture of cybersecurity awareness.