



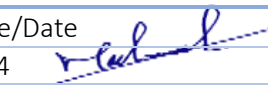
Customer Cybersecurity Awareness

Doc. Control Number	Version
SNL-06	0.3



Document Reference

Item	Description
Title	Customer Cybersecurity Awareness
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 June 2022	Muhaned Ali	First Release
0.2	16 April 2023	Muhaned Ali	Customer group has been added.
0.3	5 March 2024	Muhaned Ali	Policy has been reviewed and updated



Contents

1. Overview	4
2. Propose	4
3. Scope.....	4
4. Policy.....	4
5. Customer Group	5
6. Enforcement	5

1. Overview

The Awareness Policy bundle is a collection of policies and guidelines for the customers. This Employee Front Desk Communication Policy is part of the Social Engineering Awareness Policy bundle. To protect the assets, all customers need to defend the integrity and confidentiality of their resources.

2. Propose

Educating customers about the dangers of cyber threats helps build a stronger relationship with the customer. Stronger customers also benefit the business, since a stronger customer will reduce the risk of that customer information becoming compromised or used maliciously against your business.

An information security awareness program is defined and conducted for all customers.

3. Scope

This policy applies to all SNLC customers in the government and private sectors using data whether individually controlled or shared, stand-alone, or networked. It applies to all the customer's facilities owned, leased, operated, or contracted.

4. Policy

This policy is applicable to all SNLC customers and users of IT resources and assets.

1- Annual Information Security Awareness Training

All SNLC clients will be required to complete annual information security awareness training annually. Automatic email alerts and reminders will be sent to all customers for information security awareness.

The Awareness shall:

- Explain acceptable use of information technology.
- Inform customers about relevant policies and standards and risks to information systems.
- Educate customers on cyber security topics, including but not limited to:
 - 1- Customers should understand how to create strong passwords and learn why passwords are so important in protecting their online accounts.
 - 2- MFA implementation.
 - 3- Customers should be aware that ransomware is one of the most popular threats targeting businesses across the world.
 - 4- Removable media such as USB drives, external hard drives, and other portable storage devices can be a major risk for your organization.
 - 5- Virus or malicious software (Malware).
 - 6- Phishing attempts.
 - 7- Vishing
 - 8- Social engineering.
 - 9- Safe Web Browsing
 - 10- Application / Operating system vulnerabilities.
 - 11- Physical security.
 - 12- Incident Reporting



5. Customer Group

- 1- Customers of SNLC can be classified as follows:
 - Oil & Gas
 - Government sector
 - Private sector
- 2- Customer cyber security awareness should be conducted on a quarterly basis.

6. Policy Review

This policy will be reviewed and updated annually to ensure it remains relevant and effective in addressing evolving cybersecurity threats and best practices.

7. Enforcement

AS per CST requirements, SNLC will Enforce this policy on all customers.