Network Security Policy

Doc. Control Number	Version
SNL-17	0.3

Document Reference

Item	Description
Title	Network Security Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	25 March 2024
Revision-Date	25 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	25/3/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	25/3/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	25/3/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	18 Jan 2022	Muhaned Ali	First Release
0.2	28 May 2023	Muhaned Ali	Protect the Information Transferred has been added.
0.3	25 March 2024	Muhaned Ali	The policy has been reviewed

Contents

1. Purpose

This policy establishes the guidelines and principles for ensuring the security, integrity, and availability of SNLC's network infrastructure. The objective of this policy is to safeguard critical information assets, prevent unauthorized access, and mitigate potential threats and vulnerabilities within the SNLC's network environment.

2. Scope

This policy covers all SNL computing, networking, infrastructure, and information resources.

3. Policy

3.1 Managing and Controlling Network Security

a) SNLC is committed to managing and controlling the security of all networks operated by the company and the information assets connected to them.

b) Implement security measures to protect against unauthorized access, data breaches, and other network-related risks.

c) Use techniques such as firewalls, intrusion prevention systems (IPS), and network segmentation to control traffic flow.

d) Firewalls must be implemented at the network perimeter and only required services must be allowed. Vulnerable services or insecure protocols should be blocked.

3.2 Network Segregation

a) Segregate networks based on the criticality of information assets and services, isolating production, development, testing, and user workstations.

b) Establish clear boundaries to prevent unauthorized communication between network zones.

c) Limit communication between segments based on business needs and security requirements.

d) Servers and workstations subnets must be segmented and access between them is restricted and monitored.

e) Servers accessible from the Internet must be placed in a DMZ (i.e., perimeter network) with restricted access to internal subnets.

3.3 Security Requirements for Network Services

a) Implement security measures to protect network services and the information transferred through them, ensuring confidentiality, integrity, and availability.

b) Use appropriate security protocols, encryption, and access controls to safeguard data in transit.

3.4 Wireless Network Security

a) Secure wireless networks with strong encryption protocols (e.g., WPA3) and ensure proper authentication methods.

b) Regularly monitor and audit wireless network access points for unauthorized connections.

c) Personal/Guest devices must not be connected to any corporate Wi-Fi. Any personal device which is audited as being connected to corporate Wi-Fi will immediately be blocked.

3.5 Remote Access and VPNs

a) Implement secure virtual private network (VPN) connections for remote access.

b) Enforce multi-factor authentication (MFA) and strong encryption for remote connections.

3.6 Network Monitoring and Logging

a) Deploy network monitoring tools to detect and respond to suspicious activities and anomalies.

b) Control incoming and outgoing network traffic to prevent malicious activities, monitor traffic loads, and manage unwanted communication.

c) Collect and retain network logs for forensic analysis, incident investigation, and compliance audits.

d) Network connections to information systems and applications at the SNLC location must be authorized and monitored.

3.7 Patch Management

a) Regularly update and patch network devices, including routers, switches, and firewalls, to address known vulnerabilities.

b) Establish a patch management process to ensure timely updates without disrupting operations.

3.8 Network Device Configuration

a) Network devices should be configured securely, with unneeded services disabled and strong passwords used, in accordance with the SNLC baseline configuration.

b) Implement least privilege access for device management.

3.9 Denial of Service (DoS) Protection

a) Employ DoS protection mechanisms to prevent or mitigate attacks aimed at overwhelming network resources.

b) Implement measures to detect and prevent Distributed Denial of Service (DDoS) attacks and other abnormal traffic patterns.

c) Collaborate with other organizations operating interconnected networks to detect and prevent malicious acts such as email spam, DDoS attacks, and abnormal traffic patterns.

3.10 Network Device Hardening

a) Follow industry best practices and vendor recommendations to harden network devices against potential attacks.

b) Adhere to the SNLC baseline configuration.

3.11 Documentation of Network Plan

a) Maintain an up-to-date Network Plan that accurately reflects the network's architecture, connections, and critical servers.

b) Ensure that the Network Plan serves as a reliable reference for network management and security assessment.

3.12 Boundary Control and Protocol Management

a) Allow only trusted and authorized protocols and IP address ranges to cross network boundaries using firewalls.

b) Disable unused protocols and features on network equipment to minimize the attack surface.

3.13 Data Protection and Encryption

a) Protect information transferred through the SNLC's network using encryption mechanisms to maintain confidentiality and integrity.

b) Apply encryption to sensitive data and communications, especially in public or unsecured environments.

4. Policy Review

4.1 This policy will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this policy shall be communicated to all relevant employees and stakeholders.

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.