



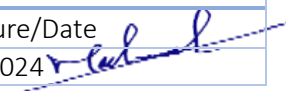
Risk Treatment and Monitoring Policy

Doc. Control Number	Version
SNL-69	0.2



Document Reference

Item	Description
Title	Risk Treatment and Monitoring Policy
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	11 March 2024
Revision-Date	11 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	11/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	11/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	11/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	11 March 2024	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Purpose	4
2. Scope	4
3. Risk Treatment Plan	4
4. Risk Monitoring Plan	4
5. Compliance.....	5

1. Purpose

The purpose of this policy is to establish guidelines and procedures for the effective treatment and monitoring of cybersecurity risks within SNLC. This policy outlines the requirements for developing and implementing risk treatment plans and risk monitoring plans to mitigate potential threats and vulnerabilities.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who have access to SNLC's information systems, networks, and data assets.

3. Risk Treatment Plan

3.1 Risk Identification and Assessment

- a) All potential cybersecurity risks shall be identified and assessed using standardized methodologies, such as the NIST Cybersecurity Framework or ISO/IEC 27001.
- b) Risks shall be evaluated based on their likelihood of occurrence, potential impact, and severity.

3.2 Risk Mitigation Strategies

- a) A risk treatment plan shall be developed for each identified risk, outlining specific mitigation strategies and controls.
- b) Mitigation strategies shall be tailored to address the unique characteristics and requirements of each risk.

3.3 Resource Allocation

- a) Adequate resources, including financial, human, and technological, shall be allocated to implement and sustain risk mitigation measures.
- b) Resource allocation shall be aligned with organizational priorities and risk tolerance levels.

3.4 Implementation Timeline

- a) Clear timelines and milestones shall be established for the implementation of risk mitigation measures.
- b) Progress shall be monitored regularly to ensure timely completion of risk treatment activities.

3.5 Communication and Stakeholder Engagement

- a) Open communication channels shall be maintained with relevant stakeholders, including executive leadership, IT teams, and external partners.
- b) Regular updates on the status of risk treatment initiatives shall be provided, and feedback shall be solicited to enhance effectiveness.

4. Risk Monitoring Plan

4.1 Continuous Risk Assessment

- a) Continuous monitoring processes shall be implemented to detect changes in the cybersecurity landscape and emerging threats.
- b) Automated tools and technologies shall be utilized to collect and analyze relevant data for real-time risk assessment.

4.2 Incident Response

- a) A robust incident response plan shall be developed to address cybersecurity incidents promptly and effectively.
- b) Roles, responsibilities, and escalation procedures shall be defined to facilitate timely response and resolution of security breaches.

4.3 Performance Metrics and KPIs

- a) Measurable KPIs shall be defined to assess the effectiveness of risk mitigation measures and overall cybersecurity posture.
- b) KPIs shall be monitored regularly, and risk management strategies shall be adjusted as needed to address evolving threats.

4.4 Reporting and Documentation

- a) Comprehensive reports on the status of cybersecurity risks, including identified threats, mitigation efforts, and outcomes, shall be generated.
- b) Documentation shall be accurate, accessible, and regularly updated to facilitate informed decision-making and compliance with regulatory requirements.



5. Compliance

- a) Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.