



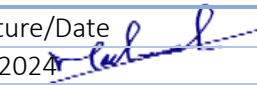
# Vulnerability Management Policy

Doc. Control Number	Version
SNL-15	0.3



## Document Reference

Item	Description
Title	Vulnerability Management Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	13 March 2024
Revision-Date	13 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	13/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	13/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	13/3/2024 

## Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	13 Jan 2022	Muhaned Ali	First Release
0.2	9 July 2023	Muhaned Ali	The policy has been reviewed and updated
0.3	13 March 2024	Muhaned Ali	The policy has been reviewed and modified



## Contents

1. Overview .....	4
2. Scope .....	4
3. Policy .....	4
4. Compliance and Enforcement .....	5
5. Policy Review .....	5

## 1. Overview

This policy establishes guidelines for the effective management of vulnerabilities within SNLC. The policy defines the scope of vulnerability management activities, tools, and technologies to be utilized, reporting requirements, frequency of scans, and timeframes for remediating vulnerabilities based on their criticality. These measures are implemented to proactively identify and address vulnerabilities to minimize the risk of exploitation and ensure the security of SNLC's systems and data.

## 2. Scope

The vulnerability management program shall cover all systems, networks, applications, and infrastructure components within SNLC.

External-facing systems, critical infrastructure, and high-risk assets shall receive prioritized attention in vulnerability management efforts.

## 3. Policy

### 3.1 Tools and Technology

- a) SNLC shall utilize industry-standard vulnerability scanning and assessment tools to identify vulnerabilities.
- b) The tools and technologies employed should be capable of identifying common vulnerabilities, misconfigurations, and emerging threats.
- c) List of the tools that the SNLC team uses for vulnerability scanning:
  - OpenVAS
  - Nessus
  - Nmap
  - Wazuh

### 3.2 Reporting

- a) Regular reports shall be generated from vulnerability scans and assessments.
- b) Reports should provide an overview of identified vulnerabilities, their criticality, affected systems, and recommended actions for remediation.
- c) Reports shall be shared with relevant stakeholders, including system owners, IT teams, and management, as appropriate.

### 3.3 Frequency of Scans

- a) Vulnerability scans shall be conducted on a regular basis to ensure timely identification of new vulnerabilities and changes in the security posture.
- b) The frequency of scans may vary based on the risk profile and criticality of systems, with higher-risk systems undergoing more frequent scans.
- c) Critical systems may require monthly scans, while less critical systems may be scanned quarterly or semi-annually.

### 3.4 Timeframes for Vulnerability Remediation

- a) Vulnerabilities shall be prioritized based on their severity, potential impact, and the criticality of the affected systems.
- b) Timeframes for remediating vulnerabilities should be defined based on their criticality and potential risk.
- c) High-risk vulnerabilities that pose an imminent threat shall be remediated within the shortest feasible time frame.

- d) Medium and low-risk vulnerabilities shall be addressed within reasonable time frames, considering resource availability and potential impact.

Severity Level	Risk Description	Remediation Timeline
<b>Critical</b>	Critical vulnerabilities have a CVSS score of 8.0 or higher. They can be readily compromised with publicly available malware or exploits.	2 Days
<b>High</b>	High-severity vulnerabilities have a CVSS score of 8.0 or higher or are given a high severity rating by PCI DSS v3. There is no known public malware or exploit available.	20 Days
<b>Medium</b>	Medium-severity vulnerabilities have a CVSS score of 6.0 to 8.0 and can be mitigated within an extended time frame.	90 Days
<b>Low</b>	Low-severity vulnerabilities are defined with a CVSS score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented and properly excluded if they can't be remediated	180 Days
<b>Information</b>	Information vulnerabilities have a CVSS score lower than 4.0. These are considered risks but are generally reference information for the state and configuration of an asset.	Not Required

#### 4. Compliance and Enforcement

- 4.1 Compliance with this policy is mandatory for all employees and individuals responsible for system administration and security within SNLC.
- 4.2 Non-compliance with this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, and legal consequences, as appropriate.

#### 5. Policy Review

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