Penetration Testing Policy

Doc. Control Number	Version
SNL-51	0.2

Document Reference

Item	Description
Title	Penetration Testing Policy
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	16 July 2024
Revision-Date	16 July 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	7/16/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	7/16/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	7/16/204

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	16 July 2023	Muhaned Ali	First Release
0.2	16 July 2024	Muhaned Ali	The policy has been reviewed

Contents

1. Overview

This policy establishes the guidelines and procedures for conducting penetration testing within the company. It outlines the purpose of penetration tests, overall objectives, and defines the frequency of testing to ensure the identification of vulnerabilities and assessment of the company's security posture.

2. Scope

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

3. Policy

3.1 Purpose of Penetration Tests and Overall Objectives

a) Penetration tests are conducted to identify vulnerabilities in the SNLC's systems, networks, and applications that could be exploited by unauthorized individuals.

b) The overall objectives of penetration tests are to:

- Assess the effectiveness of existing security controls and mechanisms.
- Identify weaknesses in the organization's infrastructure and applications.
- Determine the impact of successful attacks on the organization's assets.
- Provide recommendations for mitigating identified vulnerabilities.
- Validate the SNLC's compliance with relevant security standards and regulations.

3.2 Defining the Frequency of Penetration Tests

a) The frequency of penetration tests shall be determined based on the SNLC's risk profile, the criticality of systems and networks, and industry best practices.

b) A regular schedule of penetration tests shall be established, taking into consideration the following factors:

- Changes to the SNLC's infrastructure, systems, or applications.
- Introduction of new technologies or significant updates to existing technologies.
- Addition or removal of critical assets.
- Changes in the threat landscape or regulatory requirements.

3.3 Penetration Testing Approaches

a) The company shall utilize different approaches to penetration testing, including:

- **External testing**: Assessing external systems and networks that are accessible from the internet.
- **Internal testing**: Assessing internal systems and networks to identify vulnerabilities that can be exploited by insider threats.
- **Application testing**: Assessing the security of applications and web services.
- **Wireless testing**: Assessing the security of wireless networks and devices.

b) The selection of the appropriate penetration testing approach shall be based on the SNLC's specific requirements, risk profile, and industry best practices.

4. Compliance

4.1 All penetration testing activities shall comply with applicable laws, regulations, and contractual obligations.

4.2 The SNLC's cybersecurity team or designated personnel shall oversee the implementation and enforcement of this policy.

4.3 Non-compliance with this policy may result in disciplinary action, including termination of employment or contract.

5. Review and Revision

5.1 This policy shall be reviewed at least annually or as deemed necessary by the SNLC's cybersecurity team to ensure its relevance and effectiveness. Any proposed revisions shall be submitted for approval before implementation.