Penetration Testing Process

Doc. Control Number	Version
SNL-52	0.2

Document Reference

Item	Description
Title	Penetration Testing Process
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	17 July 2024
Revision-Date	17 July 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	7/17/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	7/17/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	7/17/2024

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 document has been reviewed

Contents

1. Process Objective

The objective of this process is to conduct penetration testing using standard methodologies to identify unknown vulnerabilities within the company's systems, applications, and networks. It defines the scope and frequency of penetration tests, utilizes vulnerability reports to guide testing, reports the penetration test findings to respective departments for remediation actions, and ensures continuous measurement, review, and optimization of the requirements for penetration testing and the effectiveness of the process.

2. Process Guidelines

2.1 Scope and Frequency of Penetration Tests

a) Define the scope of penetration tests, considering the critical information assets and systems within the company that require testing.

b) Conduct penetration tests annually, to ensure a proactive approach to identifying vulnerabilities.

c) Adjust the frequency of penetration tests based on factors such as the risk profile, changes in infrastructure or applications, emerging threats, and industry best practices.

2.2 Penetration Testing Methodologies

a) Utilize standard methodologies, such as grey box testing and white box testing, to identify unknown vulnerabilities within the company's systems and applications.

b) Grey box testing involves testing with partial knowledge of the system's internal workings, simulating an attacker with limited insider knowledge.

c) White box testing involves testing with full knowledge of the system's internal workings, simulating an authorized user with access to source code and system details.

d) Determine the appropriate penetration testing methodology based on the specific objectives, available resources, and the company's risk profile.

2.3 Use of Vulnerability Reports as Input

a) Utilize the vulnerabilities report, generated from previous security assessments or vulnerability management activities, as an input to guide penetration testing efforts.

b) Incorporate the identified vulnerabilities into the penetration testing scope and prioritize their testing based on their severity and potential impact.

c) Validate and verify the existence of vulnerabilities identified in the report, ensuring thorough coverage of potential attack vectors.

2.4 Reporting and Remediation

a) INFOSEC prepared a comprehensive penetration test report that includes detailed findings, identified vulnerabilities, their impact, and recommended remediation actions.

b) INFOSEC report the penetration test findings to the respective departments or teams responsible for the affected systems or applications.

c) Trigger remediation actions by collaborating with the respective departments and providing support or guidance on patch management activities.

d) INFOSEC monitor the progress of remediation actions and verify the effectiveness of implemented patches or controls.

2.5 Continuous Measurement, Review, and Optimization

a) Continuously measure and review the effectiveness of the requirements for penetration testing, including the scope, methodologies, and frequency of tests.

b) Review and update the requirements for penetration testing based on emerging threats, changes in technology, regulatory requirements, and industry best practices.

c) Identify areas for process optimization, such as streamlining testing methodologies, enhancing automation tools, or improving communication and collaboration with stakeholders.

d) Regularly assess the effectiveness of the penetration testing process to ensure it aligns with the organization's security goals and objectives.

2.6 Compliance

a) All employees involved in the penetration testing process must adhere to this process.

b) Non-compliance may result in disciplinary action as per the company's policies.