This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Penetration Testing Standard Template

Choose Classification

DATE:	Click here to add date
VERSION:	Click here to add text
REF:	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual’s full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated by	Version Details
<Insert version number>	Click here to add date	<Insert individual’s full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements to test and assess the effectiveness of cybersecurity enhancement capabilities in <organization name> by simulating actual cyber-attack technologies and methods, and detecting zero-day security weaknesses that may lead to the penetration of technology assets in <organization name>.

These requirements are aligned with the Penetration Testing Policy and NCA's cybersecurity requirements including but not limited to: (ECC – 1: 2018), (CSCC – 1:2019) and other relevant legal and regulatory requirements.

Scope

This standard covers all <organization name>'s systems and its technology components as well as all externally provided services (via internet) and its technology components including; infrastructure, websites, web applications, smart phones and tablets applications, emails, remote access and ICS/OT networks environment. This standard applies to all personnel (employees and contractors) in <organization name>.

Standards

1	General Requirements
Objective	To define the general requirements and scope for the penetration testing to be followed by internal and external penetration testing team prior to initiating the penetration testing process.
Risk Implication	Ad-hoc or improperly planned penetration testing could result in insufficient or inaccurate outcomes that might impact systems efficiency.

Requirements	
1-1	A plan for penetration testing that covers in-scope systems and applications, start date, end date, methodology, and real-world attack scenarios must be developed and approved.
1-2	Penetration testing action plan must be designed based on the relevant legislative and regulatory requirements.
1-3	Penetration testing must be conducted based on a defined and approved methodology and as per the relevant legislative and regulatory requirements
1-4	Rules of engagement document must be developed prior to the test, and it must include the system owner, system administrator, main interaction controls during the test, permissions given to the test administrator, test scope, active devices and their ports and services, test type, test duration, number of the penetration testers, penetration testing mechanism, tools and techniques to be used by the internal or external penetration testers, general requirements, etc.
1-5	A report must be developed after finalizing the penetration testing activity. The report must include the following sections at minimum: • Executive Summary • Reporting Introduction • Target Assets • Vulnerability Categorization Methodology • Attack Vectors • Timeline for Assessment Activity • Tests Performed • Challenges • Detailed Findings and Recommendations

1-6	An action plan must be developed after finalizing the penetration testing report in order to implement the recommendations. The report must include the following at minimum: • Technical Owner • Business Owner • Required Actions to implement the recommendations. • Clear Deadlines to implement the recommendations.
1-7	Any user, system or workstation that was used in, or was part of, the penetration testing exercise must be controlled and monitored to ensure that they are used only for the purpose of the testing exercise.
1-8	Any user, system or workstation that was used in, or was part of, the penetration testing exercise must be removed or restored to normal behavior and access after the testing exercise.
1-9	A report must be developed for each failed or incomplete penetration testing exercise. The report must highlight the challenges faced by the test team to understand and resolve them, and redo the exercise.
2	Penetration Testing Mechanism
Objective	To define penetration testing mechanism, tools and technology to be followed by internal and external penetration testing team prior to initiating the penetration testing process.
Risk Implication	Improper penetration testing can lead to new vulnerabilities, unauthorized access or continuation of unknown vulnerabilities in the environment, which can lead to inconclusive results. In addition, it could lead to exfiltration or exposure of data that may cause damage systems, services and technology components.

Requirements	
2-1	Penetration testing must be performed periodically in accordance with <organization name>'s approved Penetration Testing Policy.
2-2	Penetration testing must be conducted for all Internet-facing systems on a scheduled and regular basis, and must follow defined and approved methodology and procedures.
2-3	Penetration testing must be conducted for all critical systems' technical components and all its internal and external services on a scheduled and regular basis (every 6 months), based on defined and approved methodology and procedures.
2-4	Penetration testing must be conducted for remote work systems at least once per year, and must follow defined and approved methodology and procedures.
2-5	Penetration testing exercise must be conducted as per the relevant legislative and regulatory requirements and must take into account the following guidelines: 2-5-1 The exercise must meet specific penetration testing requirements, which are mentioned in the procedures. 2-5-2 Previous testing reports and supporting documents such as network diagrams and technical security standard controls must be reviewed and utilized as inputs for the testing exercise to understand how a system, application or technical component functions. 2-5-3 The exercise must define the testing approach whether black box (penetration testing without providing information to the party conducting the test), white box (penetration testing with all information provided to the

	party conducting the test), or grey box (penetration testing while providing limited information to the party conducting the test). 2-5-4 The systems/applications, services, or technical components targeted for testing must be identified, as well as any system/application specific information, requirements or permissions targeted for testing. 2-5-5 Passively review and examine systems, applications, networks, policies, and procedures to discover security vulnerabilities through documentation review, log review, ruleset review, system configuration review, network sniffing, or file integrity checking. 2-5-6 Test bed or an environment that mimics critical systems or actual production environment must be created in the penetration testing and it must include, at minimum, the following: • Social Engineering • Network Level Penetration Testing • Application-Level Penetration Testing • Wireless Penetration Testing 2-5-7 Results must be documented for each step in the testing exercise

Roles and Responsibilities

1- **Standard Sponsor and Owner:** <head of the cybersecurity function>.

2- **Standard Review and Update:** <cybersecurity function>.

3- **Standard Implementation and Execution:** <information technology function>.

4- **Standard Compliance Measurement**: <cybersecurity function>.

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.