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

Insert organization logo by clicking on the placeholder to the left.

Penetration Testing Policy Template

Choose Classification

Date	Click here to add date
Version	Click here to add text
Ref	Click here to add text

Replace <organization name> on behalf of the entity for the entire document. To do this, follow the below steps:

- Press "Ctrl" and "H" keys at the same time.
- Add "<organization name>" in the Find text box.
- Enter the full name of your destination in the "Replace" text box.
- Click on "More" and make sure "Match case" is selected.
- Click "Replace All".
- Close the dialog.

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 policy aims to define the cybersecurity requirements related to assessing and testing the effectiveness of <organization name>'s defense, by simulating real attacks techniques and technologies, to discover unknown security weaknesses that might compromise <organization name>.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018 and CSCC-1:2019, in addition to other related cybersecurity legal and regulatory requirements.

Scope

This Policy covers all 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, and remote access in <organization name> and applies to all personnel (employees and contractors) in <organization name>.

Policy Statements

1 General Requirements

1-1 Rules of engagement document must be developed prior to the Penetration Testing process, which must cover the scope of testing, privileges, duration, target systems, testing mechanism, general conditions and requirements, etc.

1-2 The scope of penetration testing must include all technology components including: infrastructure, websites, web applications, smart phones and tablets applications, emails, and remote access, OT/ICS network environment in accordance with the relevant legal and regulatory requirements.

1-3 Penetration Testing must be conducted to evaluate and test the efficiency of cybersecurity capabilities regularly.

1-4 Penetration testing must be conducted on critical systems, their technology components and all their internal and external services at least every six months.

1-5 Penetration testing must be conducted on telework systems and all externally provided services (through the internet) and their technology components at least once a year.

1-6 Ensure that the testing effect is limited on the production environment (operating environment) or conduct penetration testing in a identical separate environment.

1-7 Passive testing must be conducted to review and examine systems, applications, networks, policies and procedures, and detect security vulnerabilities.

1-8 A plan for penetration testing that covers scope of work, start date, end date, methodology, and real-world attack scenarios must be developed and approved.

1-9 Ensure that the penetration testing does not impact systems and provided services in <organization name> .

1-10 A qualified team with relevant certificates and experience must be appointed to ensure effective penetration testing .

1-11 Penetration testing team must coordinate with stakeholders from <organization name> to follow the approved procedures and penetration testing plans, conduct the necessary analysis in order to define the false positive indicators, classify vulnerabilities and determine their causes.

1-12 Penetration testing data must be processed in a secure manner and must be collected, stored, transferred, and removed when it becomes unnecessary according to <organization name> Data and Information Protection Policy.

1-13 Penetration testing must be conducted to discover vulnerabilities of all forms, including vulnerabilities that usually result from application development errors without taking into account the Secure Code Development and Misconfigurations standard as well as the Exploitability of Identified Vulnerability.

1-14 If a third party is assigned to conduct penetration testing on behalf of <organization name>, third party cybersecurity requirements must be verified as per <organization name>'s Third-party Cybersecurity Policy.

1-15 A report must be developed stating the testing results, recommendations must be made after completion of penetration testing process.

1-16 Penetration testing results must be classified based on their sensitivity, and remediated according to their cyber risks as per <organization name> risk management methodology

1-17 An action plan must be developed to remediate penetration testing results and illustrate risk impacts, treatment mechanism, implementation owner, duration and monitoring.

1-18 User accounts used to conduct penetration testing must be managed and monitored to ensure that they are only used for legitimate purposes and removed after testing.

1-19 Procedures and standards for penetration testing must be developed based on business need.

1-20 Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of Penetration Testing requirements.

Roles and Responsibilities

1- **Policy Owner:** <head of the cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

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

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

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

Compliance

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

2- All personnel of <organization name> must comply with this policy.

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