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 outlined image.

Vulnerabilities Management Standard Template

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.

Choose Classification

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

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 ensure timely detection and effective remediation of technology vulnerabilities to prevent or minimize the likelihood of exploiting these vulnerabilities through cyber attacks, and to minimize the impact of these attacks on <name of organization> business, and to protect it from internal and external threats at <name of organization>.

The requirements in this standard are aligned with the Server Security Policy and 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 standard applies to all information and technology assets in <name of organization>, and to all personnel (employees and contractors) in <name of the organization>.

Standards

1	General Requirements
Objective	To define the general requirements for vulnerabilities assessment to be followed by internal and external vulnerabilities assessment team prior to conducting vulnerabilities assessment process.
Risk Implication	Ad-hoc vulnerability management could result in insufficient or inaccurate outcomes that might impact systems efficiency.
Requirements	
1-1	A plan for periodic vulnerability assessments must be developed that defines the assessment scope, start date, and end date.

1-2	Vulnerability assessment plan must be based on the relevant legislative and regulatory requirements.
1-3	Vulnerability management activity must follow a defined methodology, in accordance with <organization name>'s enterprise and cybersecurity risk management policies, procedures, and processes.
1-4	A report must be developed after finalizing the vulnerability assessment activities. The report must include the following sections at minimum: • Executive Summary • Reporting Introduction • Methodology • Target Assets • Detailed Findings of the results of the vulnerability assessment.
1-5	An action plan must be developed after finalizing the vulnerability assessment report in order to implement the recommendations. The report must have at minimum: • Technical Owner • Business Owner • Required Actions to implement the recommendations. • Clear Deadlines to implement the recommendations.
2	Vulnerabilities Assessment Approach
Objective	To define and set a plan for vulnerabilities assessment and the tools to be used to be followed by internal and external vulnerabilities assessment team prior to conducting vulnerabilities assessment process.

Risk Implication	Improper vulnerability assessment can lead to inconclusive or misleading outcomes, which might lead to exploitations of the vulnerabilities and waste of resources.
Requirements	
2-1	Vulnerability assessment must be performed periodically or at least annually.
2-2	Vulnerability assessment must be conducted on a monthly basis for all external critical systems (Internet-facing systems).
2-3	Vulnerability assessment must be conducted on a quarterly basis for all internal critical systems.
2-4	Assessing, remediating, and classifying telework systems vulnerabilities based on criticality at least once every three months.
2-5	Assessing and remediating cloud services vulnerabilities at least once every three months.
2-6	Vulnerability assessment exercise must be conducted as per the relevant legislative and regulatory requirements, and it must take into account the following guidelines: • The exercise must meet specific vulnerability assessment requirements which are mentioned in the procedures. • The exercise must define the systems/applications targeted for assessment, as well as any targeted system/application specific requirements. • The assessment must include network-related vulnerabilities, service-based vulnerabilities, and banner grabbing. • Vulnerability assessment must be performed using approved methods and mechanisms.

	• Vulnerability assessment tools must be hardened to resist unauthorized use or modification, and the tool's configuration settings must not be altered. If a tool configuration change is required, <organization name> must be notified and approve of the change. • Vulnerability assessment reports must be classified as "Secret" at least, protected by a password, and shared only with related entities. • Risk rating must be determined to prioritize findings as per the cybersecurity risk management methodology.
3	Vulnerabilities Remediation
Objective	To define a specific approach for effective remediation of vulnerabilities, prevention or mitigation of exploiting vulnerabilities, and reduction of impacts of business operation.
Risk Implication	Improper remediation of identified vulnerabilities can lead to those vulnerabilities being leveraged and used in cyber attacks.
Requirements	
3-1	An action plan for remediation, fixing the identified gaps and patching targeted systems/applications, must be developed. The plan must include vulnerabilities details, recommendations, assessment start date and end date, and the functions/teams involved in the exercise.
3-2	The vulnerability assessment action plan must be documented and approved by <organization name>.
3-3	All systems and devices within <organization name> must have vendor/manufacturer warranty as per the Service Level Agreement with the vendor/manufacturer.

3-4	All systems and devices within <organization name> should have up-to-date security patches at the operating system and application level.
3-5	Automated tools for updating operating systems and software (including third party software) are encouraged to be deployed in the environment.
3-6	Critical vulnerabilities must be patched immediately after their discovery as per <organization name> change management procedures. Any high or medium risk vulnerabilities should have a priority in the action plan and be closed and remediated within a maximum of two weeks from releasing the fix or patch from the vendor, unless there is business or technical justification that is communicated officially.
3-7	The vulnerabilities sent by the Cloud Service Provider to <organization name> must be managed and remediated.

Roles and Responsibilities

1- **Standard 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.