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 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 4
Scope 4
Policy Statements 4
Roles and Responsibilities 7
Update and Review 7
Compliance 7

Purpose

This policy aims to define the cybersecurity requirements related to ensuring that technical vulnerabilities are detected in a timely manner and effectively remedied to prevent or reduce the exploitation of these vulnerabilities by cyberattacks, as well as mitigating their impact on <organization name>'s business and protecting it from internal and external threats.

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

Scope

This policy covers all <organization name>'s information technology assets and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1- General Requirements

1-1 Vulnerabilities must be scanned and assessed on a regular basis by a competent and qualified team to detect and assess technical vulnerabilities in a timely manner and remedy them effectively according to the relevant legal and regulatory requirements as follows:

Asset Type	Systems					
	All systems	Critical systems connected to the internet	Internal critical systems	Telework systems	Social media accounts systems	Cloud Computing Service Systems
	Frequency of vulnerability scanning and assessment					
Operating Systems	Monthly	Monthly	Monthly	Monthly	Monthly	Monthly

Databases	3 months	Monthly	3 months*	Monthly	Monthly	3 months
Network Devices	3 months	Monthly	3 months*	Monthly	Monthly	3 months
Applications	3 months	Monthly	3 months*	Monthly	Monthly	3 months

* The vulnerability scanning must be monthly, while the vulnerability assessment must be every three months.

1-2 Define systems, services, and technology components to be subject to vulnerability assessment as per the relevant legal and regulatory requirements.

1-3 Use reliable and approved methods and tools to detect vulnerabilities.

1-4 Assess vulnerabilities before publishing services or systems online, or upon any change to infrastructure or systems as per Cybersecurity in Information Technology Projects Policy approved by <organization name>.

1-5 Classify vulnerabilities as per risk level and remedied in line with the resulting cyber risks and <organization name>’s Risk Management Methodology.

1-6 If a third party is assigned to conduct vulnerability assessment on behalf of <organization name>, third party cybersecurity requirements must be verified as per Third-party Cybersecurity Policy approved by the <organization name> and the relevant legal and regulatory requirements.

1-7 Communicate and subscribe with authorized and trusted cybersecurity resources “Threat intelligence", special interest groups and external subject matter experts to collect information about new threats and how to reduce potential vulnerabilities, in addition to participation with NCA via Haseen Platform. NCA approval is required upon subscription with other providers.

1-8 In case of <organization name>'s subscription with other service providers to be informed of the latest vulnerabilities, the processes

related to the receipt, analysis and remediation of vulnerabilities from internal and external sources must be developed.

1-9 Remedy all vulnerabilities as per their severity and classification according to the cybersecurity risk management framework adopted in <organization name>.

1-10 Develop a vulnerability management plan in <organization name> which will be overseen by an internal or external vulnerability assessment team.

1-11 Define a specific approach for effective remediation of vulnerabilities, prevention or mitigation of exploiting vulnerabilities, and reduction of impacts on business operation.

1-12 Maintain records of vulnerability assessments, updates and associated changes.

1-13 Develop procedures and standards for vulnerabilities assessment based on the work need.

1-14 Key performance indicators must be used to ensure the continuous improvement of vulnerabilities management requirements.

2- Vulnerabilities Remediation Requirements

2-1 Upon finalizing the vulnerability assessment, a report must be prepared to illustrate detected vulnerabilities, classification, and recommended remediation.

2-2 After vulnerability assessment report is sent and vulnerabilities are remedied by stakeholders, a vulnerabilities assessment must be conducted again to ensure remediation.

2-3 Patches from reliable and secure sources must be used as per Patch Management Policy.

2-4 Newly detected critical Vulnerabilities must be fixed as per ‘s Change Management Procedures approved by <organization name>.

2-5 Vulnerabilities reported by the cloud computing service provider must be managed and remedied.

2-6 A Rollback Plan must be developed and implemented if patches adversely affect performance of systems, applications, or services.

2-7 If vulnerabilities are not remedied or fixed for any reason, other controls must be implemented such as disabling the compromised service, or providing compensating controls such as firewall access control and similar solutions, monitor vulnerabilities for actual attacks and report such vulnerabilities and exploits to incident response team.

Roles and Responsibilities

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

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

3- **Policy Implementation and Execution:** <IT 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 regulatory requirements.

Compliance

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

2- All personnel at <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.