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.

Malware Protection 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> 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 policy aims to define the cybersecurity requirements related to the protection of <organization name>'s information and technology assets against malware to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all <organization name>'s information and technology assets (such as workstations, mobile devices, and servers) and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1 General Requirements

1-1 <organization name> must provide appropriate, modern, reliable, and advanced protection mechanisms and techniques.

1-2 Protection mechanisms and techniques must be implemented and securely managed to protect workstations, mobile devices, servers, systems, and applications against malware.

1-3 Protection mechanisms and techniques must detect all types of malware (such as viruses, trojan horses, worms, spyware, adware, rootkits, and other types of malware).

1-4 Prior to selecting protection mechanisms and techniques, compatibility and secure integration with <organization name>'s operating and information systems, such as Windows, UNIX, Linux, Mac, and others, must be ensured.

1-5 Protection solution updates must be tested in a separate environment, other than the operation and production

environments, to ensure their safety before implementing them in the production environment.

1-6 Protection solutions must be capable to restore the definitions to a previous version if the update damages the systems or business requirements.

1-7 Access and identity procedures related to managing and operating protection solutions and their activities (e.g., disabling, modifying, etc.), must be implemented, limited to malware protection solution administrators, and reviewed periodically in accordance with the relevant approved policies in <organization name>.

1-8 Uninstalling, disabling, or reconfiguring protection solutions must be restricted and limited to protection solutions administrators only.

1-9 <cybersecurity function> must ensure the cybersecurity awareness of all personnel and educate them to handle malware and mitigate their risks.

1-10 Key Performance Indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of the protection requirements of workstations, servers, and third parties against malware.

2 Malware Protection mechanisms and techniques Configuration

2-1 Protection mechanisms and techniques configuration must be according to <organization name>'s approved technical security standards taking into account the vendor's guidelines and recommendations.

2-2 Antivirus solutions must be configured on email servers to scan all inbound and outbound emails.

2-3 Antivirus solutions must be configured on email servers to restrict receiving or sending email attachments depending on file type and content.

2-4 Antivirus solutions must be regularly updated as per <organization name>'s approved Patch Management Policy.

2-5 Updating is required for end-point devices to function.

2-6 Availability of protection solution servers must be guaranteed. Protection solutions must be compatible with the backup environment dedicated for non-critical functions and business.

2-7 Email messages must be filtered using modern protection solutions.

2-8 Access to websites and other online resources known to host malware must be prevented using a web content filtering solution.

2-9 All protection mechanisms and techniques must be synchronized centrally and with a reliable source.

2-10 Protection solutions must be configured to inspect suspicious content in separate environments, such as a sandbox.

2-11 Workstations and servers must be scanned periodically to ensure that they are malware-free.

2-12 Storage media must be scanned in a dedicated environment before their use if they are from outside <organization name>, or if they belong to <organization name> and are used on non-<organization name> systems, or by using the file and link scan feature on the National Portal for Cybersecurity Services "Haseen".

2-13 The use of external storage media in the production environment must be restricted unless secure mechanisms are developed and implemented for data transfer to the production environment.

2-14 The use of removable storage media must be restricted, and the required authorizations must be obtained before their use.

2-15 Physical and logical restriction, segmentation, and separation must be implemented when connecting <organization name>'s systems and devices to external networks, such as the Internet, remote access, or wireless connection.

2-16 Protection solutions must be automatically updated upon the release of any vendors' new versions, subject to Patch Management Policy.

2-17 Protection solutions must be provided, implemented, and securely managed to protect email and Internet browsing against Advanced

Persistent Threats (APTs) that usually use zero-day malware and viruses.

2-18 Protection solutions must be provided to detect and scan command execution.

2-19 Protection solutions must be provided to detect and scan new communication sessions.

2-20 Protection solutions must be configured to whitelist a specific list of application and program execution files to run on system servers and devices (including servers and end-points).

2-21 All workstations and servers must be protected with the end-point protection solutions approved by <organization name>.

2-22 Periodic reports on malware protection status and indicating the number and status of devices and servers running protection solutions (such as updated, outdated, or not connected, etc.) must be prepared and submitted to the <head of cybersecurity function>.

2-23 Protection solutions must be centrally managed and constantly monitored.

Roles and Responsibilities

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

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

3- **Policy Implementation and Execution:** <information technology organization> and <cybersecurity 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- <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.