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 placeholder to the left.

Malware Protection 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

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

Version Control

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

Review Table

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

Table of Contents

[Purpose 4](#_Toc110937543)

[Scope 4](#_Toc110937544)

[Standards 4](#_Toc110937545)

[Roles and Responsibilities 11](#_Toc110937546)

[Update and Review 11](#_Toc110937547)

[Compliance 11](#_Toc110937548)

# [Purpose](#_Purpose" \o "This section clarifies the importance and reasons for the development and adoption of this standard. This section also describes the standard's relationship with the requirements of NCA ECC, and organizational, legal, and regulatory requirements)

This standard aims to define the detailed cybersecurity requirements related to the protection of‏ ‏ <organization's name>'s ‏information technology assets against malware to minimize cybersecurity risks resulting from internal and external threats at <organization's name> in order to preserve confidentiality, integrity and availability.

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

# [Scope](#_Scope" \o "This section of the standard template aims to identify the assets, parties and persons to which this standard applies)

This standard covers all <organization name>’s information and technology assets (e.g., workstations, mobile devices, and servers) and applies to all personnel (personnel and contractors) in the <organization name>.

# Standards

|  |  |
| --- | --- |
| 1 | Malware Protection Solution Implementation |
| Objective | To ensure the protection of <organization name>’s information system and processing facilities including workstations and infrastructure by implementing protection solutions. |
| Risk Implication | The lack of protection mechanisms and techniques is a main cause for violating the confidentiality, integrity, and availability of data, applications, and operating systems because of different malware infecting <organization name>'s information processing facilities. |
| Requirements | |
|  | Malware protection solutions must have the following capabilities:   * Malware Prevention * Malware Detection |
|  | Malware protection solutions must have the capabilities to protect against different varieties of malware including but not limited to:   * Viruses * Worms * Trojan Horses * Spyware * Zero-Day malware * Ransomware * Keylogger |
|  | Malware protection solutions must be configured to protect the end-points of <organization name>’s information and technology assets, including:   * Firewalls * Email servers * Web servers * Proxy servers * Remote-access servers * Workstations * Mobile devices * DNS * DHCP |
|  | Each protection solution must have a central console. This will ensure a consistent implementation of Malware Protection Policy across all end-points, and continuous monitoring of malware threat. |
|  | Malware protection must be comprised of one or multiple tools that provide the functions of:   * Antivirus Software * Intrusion Prevention System * Firewalls * Content Filtering/Scanning * Application Whitelisting * Sandboxing * EDR * Network Intrusion Prevention System (NIPS) and Host Intrusion Prevention System (HIPS) * Host Intrusion Detection System (HIDS)   The functions of protection solutions must be determined based on the outcomes of the risk assessment process. |
|  | Malware detection and prevention events must be sent to the central protection solution and to the central event and log management solution for analysis, correlation, decision-making and application of automation as much as possible. |
|  | Malware defensive mechanisms must be also implemented to reduce the impact of malware threats should they occur. Those mechanisms include:   * BIOS protection. * Application sandboxing. * Browser segregation for corporate and non-corporate applications. * Segregation through virtualization. * Restriction of the automatic activation of a downloaded file, shareware, or freeware. * Restriction of end-user’s privileges on the device they use (without administrative rights). * Restriction of the automatic activation or use of macro files. * Denial of booting systems from diskettes or CDs except in case of an emergency and when using verified media. * Configuration of all software to warn the user in case documents with macros are opened. * Disabling of workstation-workstation communication. |
|  | Uninstallation of a protection solution’s agent must be password protected and remotely managed to ensure that end-users are unable to uninstall the agent, change its settings, or deactivate it and enable alert and logging. |

|  |  |
| --- | --- |
| 2 | Malware Protection Solution Configuration |
| Objective | To ensure the proper configuration is applied to protection mechanisms and techniques for effective protection against malware threats. |
| Risk Implication | Inadequate configuration of protection solutions will result in undetected malware spreading into the <organization name>’s environment and therefore reduced overall effectiveness of the solutions. |
| Requirements | |
|  | The malware protection solution's agent must be configured to perform a real-time scan on all files when they are accessed, copied, or transferred and executed. This will ensure the detection of all malwares before activation. |
|  | The malware protection solution's agent must be configured to perform a full system scan at least once a week. The time of scanning can be either when the system boots up or during non-peak usage hours. |
|  | Malware scanning must be enabled for removable media automatically when these media are inserted or connected. |
|  | Devices must be configured to not auto-run, execute, or download. |
|  | DNS query alerting and logging must be enabled to detect queries for known malicious DNS domains. |
|  | Operating system anti-exploitation and alerting and logging features must be enabled to detect and/or prevent suspicious and malicious activities. |
|  | The malware protection solution must be configured to firstly detect then respond to the malware in dedicated environment as follows: disinfect, delete, quarantine, or encrypt malware upon detection. |
|  | The malware protection solution's agent must be configured to quarantine virus-infected files if they cannot be cleaned. |
|  | The malware protection solution’s agent must be configured to notify the user if it is unable to clean or quarantine the malicious code detected on the machine. |
|  | Malware protection solutions must be installed on email servers including SMTP gateway. Protection solutions must be configured to scan email content and attachments in all emails. If malware is found in an incoming SMTP mail, then the following actions must be taken:   * Infected attachments must be cleaned. * Infected attachments must be quarantined if cleaning them is not possible. * Follow incident response procedures |
|  | Operating system and applications on the protection solution’s central console must be configured as per the relevant vendor's secure configuration guidelines. |
|  | Access to websites and other resources on the Internet known to host malicious content must be prevented using a web content filtering mechanism. |
|  | <organization name> must carry out performance monitoring for the following:   * CPU Utilization * Memory Utilization * Network Performance * Disk Utilization |
|  | Malware protection solutions' administrators must submit periodic reports on a monthly basis on the status of malware protection to <organization name>’s <cybersecurity department>. The report must include the following at a minimum:   * Number of PCs, servers, laptops, and systems not updated with the latest signature patterns. * Top 10 detected malware. * Number of viruses/worms/malicious programs detected. * Number of viruses/worms/malicious programs cleaned/quarantined/deleted. * Action taken to resolve the malware infection. * Source of infection. |

|  |  |
| --- | --- |
| 3 | Malware Protection Solution Updates |
| Objective | To ensure that protection mechanisms and techniques are up to date to protect the information and technology assets against the latest known malware. |
| Risk implication | The latest known malware might pass undetected and compromise <organization name>'s cybersecurity if the protection mechanisms and techniques are not updated. |
| Requirements | |
|  | Malware protection solutions must be automatically updated on a regular basis as per the Patch Management Policy. |
|  | Malware protection solutions must be periodically verified for integrity. |
|  | Malware protection solutions' signature database must be automatically or manually updated on a regular basis. |
|  | Malware protection solutions must be configured to acquire the signature pattern from the trusted vendor's website. |
|  | Malware protection solutions must be configured to "push" the latest signature updates to all workstations and servers while notifying the system administrator if the signatures fail to update . |
|  | Systems which are not on ‏ <organization name>'s mobile device network must be configured with alternative update options whereby the signatures can be directly updated from the trusted vendor's website. ‏ |
|  | Malware protection solutions must support signature update rollback in case the current latest updates make the antivirus software inconsistent and incapable of operating as expected. |
| 4 | Tracking New Threats and Vulnerabilities |
| Objective | To ensure the early detection of new threats that could affect the security of <organization name> and taking adequate measures to mitigate associated risks. |
| Risk implication | <organization name> could face a cybersecurity breach because of the inability to detect new and unknown malware. |
| Requirements | |
|  | <organization name> must keep track of new threats arising from malicious code and must maintain a list of the possible infection scenarios (e.g., how and in what way the virus can affect ‏ <organization name>’s information and technology assets). ‏ ‏ |
|  | The malware protection solution must be configured to identify and respond to malware based on clearly identified use cases. |
|  | When a new vulnerability is published, <organization name> ‏ must identify the steps that need to be taken to ensure that the associated risks are mitigated. |
|  | Must keep monitoring the behavior of the software and the applications most used in <organization name> to detect suspicious behavior before spreading. ‏ |

# [Roles and Responsibilities](#_Roles_and_Responsibilities" \o "This section aims to identify the roles and responsibilities related to this standard)

1. **Standard Owner:** <head of the cybersecurity function>
2. **Standard Review and Update:** <cybersecurity function>
3. **Standard Implementation and Execution:** <information technology organization> and <cybersecurity function>
4. **Standard Compliance Measurement:** <cybersecurity function>

# [Update](#_الالتزام_بالسياسة) and Review

<Cybersecurity function> must review the standard at least once a year or in case any significant technical changes occur in the infrastructure or changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements

# [Compliance](#_Compliance" \o "This section aims to identify the requirements for compliance with this standard and the consequences of incompliance)

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.