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.

# Virtualization Security Standard 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 standard aims to define the detailed cybersecurity requirements related to virtualization within <organization name>. Virtualization must be understood as a process of creating and running a virtual instance of a computer system in a layer simulated virtual environment.

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, CSCC-1:2019 and CCC-1:2020, in addition to other related cybersecurity legal and regulatory requirements.

# Scope

The standard covers <organization name>'s information and technology assets and applies to all personnel (employees and contractors) in <organization name> and related third parties.

# Standards

| 1 | Host Security |
|---|---|
| Objective | The host used for virtualization must be securely managed, and appropriately used when required. |
| Risk Implication | Host compromise may have a crucial security implication for all virtualization environments and may cause an information theft, unauthorized access, and information disclosure. |
| Requirements | |
| 1-1 | All security updates must be installed on the host OS (if present) once they are released by the vendor. All unnecessary applications, other than hypervisor, must be removed. |
| 1-2 | Host OS must be consistent with the requirements of <organization name>'s Event Log Management and Monitoring Standard and must specially gather in audit log file |

| | |
|---|---|
| | events related to failed and successful login to administration interfaces. |
| 1-3 | Physical access to the server must be restricted only to authorized employees (least privilege assignment for different administrators). |
| 1-4 | Administrative access to the management interface of the hypervisor must be restricted. |
| 1-5 | All management communication channels using a dedicated management network, or the management network communications must be protected from abuse, authenticated and encrypted using cryptographic modules compliant with National Cryptography Standard. |
| 1-6 | Unused physical hardware must be disconnected from the host system. |
| 1-7 | Unused Network Interface Controllers (NICs) must be disconnected from all networks. |
| 1-8 | The host system must be synchronized to a trusted authoritative time server. |
| 1-9 | Only Measured Launch Environment (MLE) supporting hardware must be used to establish the root of trust between the hardware and hypervisor. |
| 1-10 | Hardware must support an MLE with standard-based cryptographic measurement capabilities and storage devices. |
| 1-11 | The isolation of processes running in Virtual Machines (VM) must meet the following guidelines:<br>● The privileged commands or instructions from a Guest Operating System (Guest OS) to the host processor must be mediated to maintain Virtual Machine Manager (VMM)/hypervisor as the controller of virtualized resources. |

| | |
|---|---|
| | • The integrity of the memory management function of the hypervisor host must be protected against cybersecurity attacks such as buffer overflow and unauthorized code execution, especially in the presence of translation tables that are needed for managing memory access by multiple VMs.<br>• Memory allocation algorithms must ensure that payloads in all VMs are able to perform their functions.<br>• CPU allocation algorithms must ensure that payloads in all VMs are able to perform their functions. |
| 1-12 | All guest OSs' security tools must be monitored and managed in a predefined manner following this standard. |
| 1-13 | For side channel attacks prevention, the following mechanisms must be followed:<br>• Simultaneous multithreading (SMT) deactivation,<br>• Not using memory deduplication (if possible),<br>• Usage of processors with exclusive cache (if possible), Address space layout randomization activation. |
| 1-14 | Virtualized host migration between physical or virtual environments must follow all security requirements specified in this standard. |
| 2 | Hypervisor Security |
| Objective | The use of the hypervisor in <organization name> must be properly configured and securely managed. |
| Risk Implication | Hypervisor is the foundation of each virtual infrastructure, and any misconfiguration may have severe implications that would lead to information theft, unauthorized access, and information disclosure. |
| Requirements | |

| | |
|---|---|
| 2-1 | <organization name> must follow the best practices for managing the physical OS, e.g., time synchronization, log management, authentication, remote access, etc. |
| 2-2 | Hypervisor's installation images must be obtained from trusted sources only. |
| 2-3 | If possible, hypervisor must be installed on bare metal to avoid complexity and potential vulnerabilities present on host OS. |
| 2-4 | All updates to the hypervisor must be installed within an <organization name>'s defined time period after they are released by the vendor. |
| 2-5 | The hypervisor itself must be carefully monitored by the administrators using dedicated security tools for any signs of compromise. |
| 2-6 | Hypervisor must provide a virtual interface to the hardware based MLE. |
| 2-7 | The administration of all hypervisor installations in the enterprise must be performed centrally using an enterprise virtualization management system (EVMS). |
| 2-8 | Enterprise gold-standard hypervisor configurations for different types of workloads and clusters must be enforced through EVMS.<br>The gold-standard configurations must, at the minimum, cover the following aspects:<br>• CPU<br>• Memory<br>• Storage<br>• Network bandwidth and Host OS hardening (if required) |
| 2-9 | All hosts' OS must be completely isolated (physically and logically) from a hypervisor instance. |

| 3 | Guest OS Security |
|---|---|
| Objective | The guest OS must be securely managed and maintained ensuring independence of other systems using encapsulation and traditional security methods due to directly access to the network. |
| Risk Implication | If a guest OS on a hosted virtualization system is compromised, that guest OS may potentially infect other systems on the same hypervisor, that would lead to information theft, unauthorized access, and information disclosure. |
| Requirements | |
| 3-1 | <organization name> must follow the best practices for managing the physical OS, e.g., time synchronization, log management, authentication, remote access, etc. |
| 3-2 | All updates to the guest OS must be installed promptly. All modern OSs have features that will automatically check for updates and install them. |
| 3-3 | The virtual drives used by the guest OS on a regular basis must be backed up using the same policy for backups as is used for non-virtualized computers in <organization name>. |
| 3-4 | In each guest OS, unused virtual hardware (especially virtual drives and virtual network adapters) must be disconnected. |
| 3-5 | Separate authentication solutions for each guest OS must be used unless there is a particular reason for two guest OSs to share credentials. Authentication approval must be obtained only for a limited amount of time. |
| 3-6 | Virtual devices for the guest OS must be associated only with the appropriate physical devices on the host system, such as the mappings between virtual and physical NICs. |

| | |
|---|---|
| 3-7 | Guest OS must have access only to its own resources and must not encroach on the other guest OSs' resources or any resources not allocated for virtualization use. |
| 3-8 | Guest OS's snapshots must be restricted to prevent unauthorized disclosure. |
| 4 | Virtualized Infrastructure Security |
| Objective | Proper specification of virtualized infrastructure must be ensured in the security area. |
| Risk Implication | Misconfiguration or any violation in infrastructure virtualization may have severe implications that could lead to information theft, unauthorized access, and information disclosure. |
| Requirements | |
| 4-1 | Access to virtual hardware must be strictly limited to the guest OS that will use it. |
| 4-2 | Access control to the virtual hardware, particularly storage and networking, must be applied and strictly monitored by the administrators using dedicated security tools. |
| 4-3 | If possible, virtual network switches which support virtual LAN (VLAN) and firewall capabilities must be used to provide separation and isolation of the VM network traffic. |
| 4-4 | Additional security appliances (hardware or virtual) must be implemented to inspect, control, shape and monitor the VM network communications in a centralized location. |
| 4-5 | VM configuration management tools must be used to monitor and manage configuration of every VM throughout its lifecycle. |
| 4-6 | Emulation of hardware devices must only be used where complexity is manageable (e.g., USB host controller). |

| | |
|---|---|
| 4-7 | If possible, resource limits for network bandwidth and I/O bandwidth (e.g., disk read/write speeds) must be set for each VM to prevent denial of service (DOS) attack. |
| 5 | Desktop Virtualization Security |
| Objective | The usage of desktop virtualization must be strictly managed and regulated using the least privileged approach. |
| Risk Implication | When used, a virtualized desktop environment is a foundation of business daily operation and any misconfiguration or violation may cause the entity's cybersecurity policy violation and information disclosure. |
| Requirements | |
| 5-1 | Scenarios that require the enforcement of security by managed virtualization solutions and that do not require centralized management must be determined.<br>For instance, if desktop virtualization is allowed for employees' working from home, their computers do not need to have stringent security controls in contrast to those that provide access to internal databases or websites. |
| 5-2 | <organization name> must use virtualization solution that allows to deploy a managed desktop guest OS on unmanaged computers. |
| 5-3 | All updates must be installed to the guest OS on unmanaged computers as they are released by the vendor. |
| 5-4 | Users of managed guest OSs used by multiple users must be made aware that any changes made by one user may be propagated back to the main image and then appear in the images used by other users. |
| 6 | Other Standards |

| | |
|---|---|
| Objective | The Virtualization must be securely configured and appropriately used when required. |
| Risk Implication | If <organization name> is not compliant with all applicable and mandatory standards and requirements, it could lead to information theft, unauthorized access and information disclosure. |
| Requirements | |
| 6-1 | The following standards must be implemented in relevance to virtualization:<br>1. Server Security Standard<br>2. Network Security Standard<br>3. Identity and Access Management Standard<br>4. Backup and recovery management Standard<br>5. Cryptography Standard<br>6. Physical Security Standard<br>7. Secure Configuration and Hardening Standard<br>8. Event Log Management and Monitoring Standard<br>9. Malware Protection Standard |

# 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.