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.

Server 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 4
Scope 4
Standards 4
Roles and Responsibilities 9
Update and Review 9
Compliance 9

Purpose

This standard aims to define the detailed cybersecurity requirements related to the management and protection of <organization's name>'s servers in order to minimize cybersecurity risks resulting from internal and external threats.

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

Scope

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

Standards

1	Secure Access
Objective	To ensure the protection of servers and their functions against unauthorized access.
Risk Implication	Unauthorized access to servers exposes <organization name> to severe risks that can lead to data leakage or theft, service interruption, or security compromises that attackers can use to carry out further cybersecurity attacks against <organization name> and its infrastructure.
Requirements	
1-1	Access on servers must be restricted to server administrators by only allowing access to administrators' individual accounts and workstation IPs using network Access Control Lists (ACLs).

1-2	Default/non-interactive/unneeded accounts must be disabled or renamed.
1-3	Session timeout and session idle lockout must be configured in accordance with the <organization name>'s approved identity and access management standard.
1-4	BIOS bootloader passwords must be configured.
1-5	Access to critical servers must be restricted by administrators and operators to be provided through Privileged Access Workstations (PAW) only, and all administrative access must be encrypted.
1-6	Access to servers must be restricted by administrators and operators and must only be provided through a jump server or PAM. 1-6-1 A separate jump server must be used for system administrators and users. 1-6-2 The use of Multi-Factor authentication must be required for the access of jump servers used by system administrators by implementing ACLs. 1-6-3 Access to jump servers must be restricted to the accounts of authorized administrators and operators only. 1-6-4 Network access must be restricted to jump servers by implementing ACLs. 1-6-5 Jump servers must be placed in the network management zone. 1-6-6 Internet access on jump servers must be disabled. 1-6-7 Unnecessary and risky services (such as sending and receiving emails) must be disabled on jump servers. 1-6-8 All levels of logging, as well as audit trail and security logs, must be enabled locally and to a centralized event logging system.

2	Server Protection
Objective	To ensure the protection of servers against viruses, malware, Advanced Persistent Threats (APTs), Zero-Day attacks, and any other types of malicious attacks.
Risk Implication	Successful malicious attacks on servers can expose <organization name> to a security breach, unauthorized access, or data disclosure if servers are left unprotected.
Requirements	
2-1	OS and application functionality lockout must be configured with the least privilege required to operate in normal conditions. For example, changing system time manually, shutting down/restarting, editing system files, creating/modifying/deleting files, etc., must be disabled.
2-2	Application whitelisting must be enabled on servers to allow only specific applications and software to run based on need.
2-3	Application whitelisting agents must be configured so that users cannot disable the agents with the exception of administrators when performing specific administrative tasks that would require disabling application whitelisting temporarily.
2-4	A list of approved executables (exe, com, pif, etc.), software libraries (dll, ocx, etc.), scripts (ps1, bat, vbs, etc.), and installers (msi, msp, etc.) must be defined and approved to be executed by certain users as per the needs.
2-5	Application whitelisting must be implemented to use cryptographic hash rules, publisher certificate rules or path rules to allow or restrict the use of applications.
2-6	Application folders must be configured with file system permissions to prevent unauthorized modification of folder and file permissions.

2-7	Exploit protection functionality must be enabled on servers with both operating system mitigation measures and application-specific mitigation measures.
2-8	Endpoint Detection and Response (EDR), Host-based Intrusion Detection System (HIDS) and Host-based Intrusion Prevention System (HIPS) must be implemented on all servers.
2-9	Software host firewall must be implemented on all servers.
2-10	Antivirus must be implemented on all servers.
2-11	End-point protection must be implemented on all servers.
2-12	Advanced Persistent Threat agents must be implemented on all servers.
2-13	End-point device control software must be implemented on all servers to prevent the use of unauthorized devices.
2-14	Data Leakage Prevention (DLP) must be implemented where required in accordance with <organization name>'s approved Data Leakage Prevention standard.
2-15	All requirements under <organization name>'s Malware Protection Policy must be implemented.
3	**Central Management**
Objective	To define security requirements for central management to ensure that servers are managed and operated securely and that all security requirements are implemented and enforced.
Risk implication	The lack of secure management and the non-implementation of security requirements on servers increases the probability of exposure to attacks and the existence of vulnerabilities and weaknesses in <organization name>'s environment. Exploiting such vulnerabilities in malicious attacks or

	breaches can compromise the security of <organization name> 's servers and data.
Requirements	
3-1	Central management server or domain server must be configured to enforce <organization name>‘s Configuration and Hardening policies on all servers.
3-2	System configuration management tools that automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals must be deployed.
3-3	Configuration monitoring system compliant with Security Content Automation Protocol (SCAP) must be implemented to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.
4	Other Standards
Objective	To implement all server security standards and requirements to ensure the highest protection levels.
Risk implication	Failure to implement all security standards and requirements exposes <organization name> to increased server security risks.
Requirements	
4-1	The following standards must be implemented: 1- Virtualization security standard 2- Disaster recovery and backup standard 3- Cryptography standard 4- Cybersecurity event and monitoring management standard 5- Physical security standard 6- Secure configuration and hardening 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 organization>

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 employees 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.