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.

# Server Security 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 servers in order to minimize the cybersecurity risks resulting from internal and external threats in <organization name> and 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 (including servers) and applies to all personnel (employees and contractors) in the <organization name>.

# Policy Statements

## 1 General Requirements

1-1 All <organization name>'s servers must be identified, listed, and recorded under a specific operational team that is responsible for the operational and security processes as per <organization name>'s policies and other relevant legal and regulatory requirements.

1-2 Server technical security standards must be developed, documented, approved, and reviewed for the servers used within <organization name> in line with the best international practices, <organization name>'s approved policies and regulatory procedures, and other relevant legal and regulatory requirements.

1-3 Servers must be configured based on approved technical security standards before their deployment in the production environment.

1-4 Server backups must be performed regularly as per <organization name>'s approved Backup Management Policy to ensure their recovery in case of an accidental incident or damage.

1-5 Necessary security technologies must be used to securely decommission and reuse servers containing classified information as per the relevant policies and legal and regulatory requirements.

1-6 Server software including operating systems and application software must be kept up to date, and the latest security patches and fixes must be applied according to <organization name>'s approved Patch Management Policy.

1-7 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and effective and efficient use of the server protection requirements.

## 2 Server Configuration

2-1 <Organization name>'s approved secure configuration and hardening requirements must be applied.

2-2 Inactive servers and applications must be decommissioned as per the approved technical security standards.

2-3 Secure configuration and hardening for servers must be approved, reviewed, and updated <annually> and every six months for critical systems' servers.

2-4 Static passwords of servers must be changed as per <organization name>'s approved technical security standards.

## 3 Access and Administration

3-1 Access to <organization name>'s servers must be restricted to authorized users and when needed only.

3-2 Access to critical systems and servers must be restricted to System Administrators' accounts. Administrators' accounts and privileges must be reviewed periodically as per <organization name>'s approved Identity and Access Management Policy.

3-3 Access to critical systems' servers must be restricted and limited to the technical team that has privileged access and via workstations only, while prohibiting the use of laptops. These workstations must be isolated in a management network and must not be connected to any other network or service (e.g., email or the Internet).

3-4 Access to critical systems' servers must require Multi-Factor Authentication (MFA).

3-5 Factory and default accounts must be disabled or changed, and unused services and ports in the operating system must be disabled on all servers.

3-6 Data stored on servers must be protected and encrypted in line with <organization name>'s approved Cryptography Policy, based on the data classification type and according to the relevant legal and regulatory requirements.

## 4 Server protection

4-1 Outdated and unreliable servers must not be permitted to connect to <organization name>'s network. They must be put in an isolated network to install the required updates in order to minimize related cybersecurity risks that might lead to unauthorized access, malware infections, or data leakage.

4-2 Modern and advanced protection technologies and mechanisms must be used and managed securely on all servers to protect them against viruses, suspicious activities, malware, and Zero-Day attacks.

4-3 Only specific application and software execution files must be whitelisted on critical systems' servers.

4-4 The use of external storage media on servers must be restricted. <cybersecurity function>'s prior authorization must be obtained before using such media, and their secure usage must be ensured.

4-5 Servers must be installed in an appropriate area in the network structure/diagram as determined according to legal and regulatory requirements to ensure their effective management and protection.

## 5 Server Management Operational Requirements

5-1 Servers must be managed centrally in <organization name> to detect risks promptly and facilitate server management and monitoring through restricting access, patching, etc.

5-2 Servers in virtual environments must be protected and securely managed based on cybersecurity risk assessments.

5-3 Servers must be configured to forward logs to a Security Information and Event Management (SIEM) system as per <organization name>'s approved Cybersecurity Events Log Management and Monitoring Management Policy.

5-4 Clock synchronization shall be performed centrally for all servers according to an accurate, approved, and reliable source.

5-5 All the needed requirements to operate servers properly and securely must be provided, such as providing an appropriate and secure environment and monitoring and restricting physical access to server zones to the authorized personnel only.

5-6 The <information technology organization> must monitor operational servers and ensure their performance effectiveness, availability, storage sufficiency, etc.

## 6 Vulnerability Management and Penetration Testing

6-1 Servers must be periodically scanned for vulnerabilities, and discovered vulnerabilities must be remediated based on their classification and the associated cybersecurity risks, as per <organization name>'s approved Vulnerability Management Policy and according to the relevant legal and regulatory requirements.

6-2 Penetration tests must be conducted periodically on all servers, as per <organization name>'s approved Penetration Testing Policy.

6-3 Security patches and fixes must be deployed to remediate vulnerabilities and increase server efficiency and security as per <organization name>'s approved Patch Management Policy.

## 7 Server Physical and Environmental Security

7-1 Access to and exit from <organization name>'s server facilities must be monitored and controlled, using for example doors, physical locks, and modern surveillance systems.

7-2 Environmental factors such as heat, air conditioning, and smoke, as well as fire alarm systems and firefighting systems, must be monitored and controlled.

7-3 Physical isolation must be applied to servers and critical systems' networks in an access-restricted environment as per the relevant policies and legal and regulatory requirements.

7-4 Proper physical security controls must be implemented (e.g., security monitoring cameras inside and outside <organization name>'s data centers, security guards, secured cables, etc.).

# 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.