This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the right.

Network 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> on behalf of the entity for the entire document. To do this, follow the below steps:

- Press "Ctrl" and "H" keys at the same time.
- Add "<Entity>" in the Find text box.
- Enter the full name of your destination in the "Replace" text box.
- Click on "More" and make sure "Match case" is selected.
- Click "Replace All".
- Close the dialog.

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 <organization name>'s networks and network devices, to minimize cybersecurity risks resulting from internal and external threats at <organization name>.

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

Scope

This policy covers all networks and network devices in the <organization name> and applies to all personnel (employees and contractors) in <organization name>.

Policy Statements

1- General Requirements

1-1 All network devices of <organization name> must be identified, kept up to date and approved.

1-2 Leading global technical security standard controls for all network devices used in <organization name> must be identified and applied and Defence-in-Depth principle on the network must be applied.

1-3 Access to <organization name>'s networks must be managed according to Identity and Access Management Policy where connection to network is available when needed and to authorized users only.

1-4 Logs for all devices and systems of <organization name> must be enabled , recorded and maintained, as per the organization's approved Cybersecurity Event Logs and Monitoring Management Policy.

1-5 Maintain and update network design documents must be on an ongoing basis.

1-6 Configure clock synchronization must be on all servers to synchronize time from a trusted source.

1-7 Implement the requirements of all policies related to network security adopted by <organization name> must including but not limited to , the following:

1-7-1 Email security policy approved by <organization name> as per the relevant policies and legal and regulatory requirements.

1-7-2 Patch Management Policy approved by <organization name> as per the relevant policies and legal and regulatory requirements.

1-7-3 Web Application Security Policy approved by <organization name> as per the relevant policies and legal and regulatory requirements.

1-8 Key performance indicators must be used to ensure the continuous improvement and effective and efficient use of Cybersecurity Network Security requirements.

2- Network Access Controls

2-1 Develop and approve procedures must be used to grant and deny access to <organization name> networks , according to <organization name>'s Identity and Access Management Policy.

2-2 Access to network must be granted based on a request submitted by user to the <information technology function> indicating the type, duration and reasons of request.

2-3 In case of addition or amendment to firewall rules, necessary approvals must be obtained and network administrator must document the business requirements and request details in firewall system.

2-4 Username and password must be used to access <organization name>'s network according to <organization name> approved Identity and Access Management Policy.

2-5 Provide technologies necessary must be used to restrict and manage access to network services, protocols and ports.

2-6 Restrict all physical data ports must be within <organization name>'s facilities by port security or port-based authentication in order to reduce the exposure of network and possibly have unauthorized devices connect while being undetected.

2-7 Restrict and open network ports, protocols, and services must be used for remote access operations, especially on internal and critical systems as needed.

3- Third Parties Access Controls to the Network

3-1 Granting access to the <organization name> network to third parties must be subject to cybersecurity requirements mentioned in the third party's cybersecurity policy approved by <organization name>.

3-2 Secure encryption and authentication mechanisms must be used to transfer data to and from third parties.

3-3 A specified duration must be granted to third parties to access <organization name>'s network as agreed with the system owner.

3-4 User and third parties access rights must be regularly reviewed according to <organization name>'s cybersecurity policies.

3-5 Remote Access Management and Authentication (RAM) must be prevented on devices located in the organization's External-Facing Host.

3-6 Third-party personnel must be prevented from connecting to the network or WI-FI of <organization name> without vulnerabilities check in addition to updating the antivirus program, making the proper configuration and ensuring that their activities can be monitored.

4- Network Protection

4-1 Segment and segregate networks must be physically and logically using firewall and defence-in-depth mechanisms.

4-2 Segment critical systems network (VLAN) must be physically and logically.

4-3 Segregate production environment networks must be logically from testing environment network and other networks.

4-4 Monitor internal and external networks must be used for suspected activities.

4-5 Prevent connecting critical systems to the internet must be used if they are providing internal service to <organization name> and there is no need for remote access.

4-6 Segregate must be used for Voice Over IP "VOIP" network logically from data network.

4-7 Appropriate technologies must be used to secure browsing and internet connectivity through restricting use of suspicious websites., file storage/sharing and remote access websites.

4-8 Approve periodic update packages and security patches of assets in the production environment must be by the manufacturer and test them in a sandbox environment before being applied to the production environment.

4-9 Protection mechanisms must be securely implemented, managed and regularly updated to protect the internet browsing channel against Advanced Persistent Threats (APT) that contains usually viruses and zero-day malware .

4-10 Prevent connecting internal network directly to the internet. Connection must be via proxy to analyse and filter data from and to <organization name> .

4-11 Firewall list settings must be configured to explicitly prevent all types of connections between network components and allow only needed list based on user request and business needs while reviewing such lists periodically.

4-12 Mechanisms for DNS security must be implemented.

4-13 Intrusion Prevention Systems (IPS) such as IDS/IPS, HIDS/HIPS to network segments must be implemented and review them regularly.

4-14 Network Advanced Persistent Threat (APT) protection systems must be provided on the network of critical systems and update it continuously.

4-15 Distributed Denial of Service Attack (DDoS) systems on systems must be provided and updated on an ongoing basis.

4-16 Appropriate techniques to protect the channel used for networking with the cloud computing service provider must be used.

4-17 The use of network communications, services, and contact points between different zones must be restricted and limited in order to the minimum to meet operation, maintenance and safety requirements.

4-18 Firewall rules configurations must be reviewed on an annual basis, and critical systems networks firewall at least on a bi-annual basis

4-19 Blacklist of malicious IP addresses and websites must be developed, updated, and blocked.

4-20 Connecting Wi-Fi network to the <organization name> internal network must be prevented without a full study of associated risks, the use of safe authentication and encryption methods, protection of private technology assets, data confidentiality and integrity along with protection of <organization name> systems and applications.

4-21 Connecting critical systems to the <organization name> wireless network must be prevented.

4-22 Connecting devices to critical systems of local networks must be prevented before they get inspected to ensure they meet minimum security requirements for critical systems.

4-23 The internal and external network of <organization name> must be evaluated while ensuring the organization network cybersecurity risks match the risks appetite periodically at least once a year.

4-24 Appropriate techniques to decrypt the web traffic (SSL/HTTPS Inspection) must be provided.

4-25 Remote access and connection must be restricted to critical systems only when needed, while providing up-to-date and secure mechanisms, protocols, and technologies to ensure secure connection (e.g. VPN, Site-to-Site VPN).

4-26 Only whitelisting for critical systems firewall rules must be allowed.

5- Physical and Environmental Security

5-1 House network computer equipment must be in a controlled and secure environment and ensure temperature and humidity are set at a certain degree in addition to availability of uninterruptible power supply "UPS".

5-2 Physical access to network devices must be restricted to authorized users only to protect such devices against theft or tamper.

5-3 All access cases must be recorded and maintain related logs in addition to monitoring network device areas using CCTV with continuous monitoring.

Roles and Responsibilities

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

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

3- **Policy Implementation and Execution:** <information technology function> 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 legal and regulatory requirements.

Compliance

1- <head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis .

2- The <cybersecurity function> and the <information technology function> 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.