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 left.

Network Security 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

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 detailed cybersecurity requirements to protect <organization name> networks security to achieve the main objective which is minimizing cybersecurity risks resulting from internal and external threats.

These requirements are aligned with the Network Security Policy and NCA's cybersecurity requirements including, but not limited to: Essential Cybersecurity Controls ECC – 1: 2018, CSCC – 1:2019 and other relevant legal and regulatory requirements.

Scope

This standard covers <organization name>' s information technology networks systems and applies to all its personnel (employees and contractors).

Standards

1	Secure Access
Objective	To ensure the right security configuration is applied to the network security administration interfaces for effective protection against network security attacks.
Risk Implication	Inadequate configuration of network security administration interfaces solution may result in undetected attacks or compromise of network devices inside the <organization name>'s environment.
Requirements	
1-1	Secure Access for Networks must be implemented in accordance with the <organization name>'s approved identity and Access Management standard.
1-2	An access list must be configured to protect all network segments from Layer-3 IP address spoofing.

1-3	Restrict wireless network administrators' access to use dedicated Privileged Access Workstations (PAWs) or jump servers placed in an out-of-band management network, segmented from <organization name>'s network and isolated from the internet. Access through wireless network must be prohibited.
2	Network Segregation
Objective	To ensure the network design and architecture is secure and the network segments are protected according to their security level through network segregation.
Risk Implication	Networks without segregation share the same broadcast domain and devices will be able to communicate without policing or inspecting the traffic, therefore, any attack on any system could lead to serious internal threats and attacks on most systems of the network facilitating lateral movement within the network.
Requirements	
2-1	A logically and/or physically segmented network must be designed and implemented, taking into consideration business needs and enterprise architecture, and based on the principles of defense-in-depth and multi-tier architecture.
2-2	Appropriate level of security controls must be applied to different network segments based on the value and classification of information stored or processed in the network, levels of trust, business impact and associated risks.
2-3	Multi-tier architecture protected by dual layer of firewalls must be implemented. Specifically, the network must be segmented into three or more layers (boundary/perimeter, core and trusted) and the network segments must be divided into zones (demilitarized zone "DMZ", management zone, production zone, database zone, development/testing zone, etc.) as per

	<organization name>'s enterprise architecture and security architecture.
2-4	Networks must be designed and configured to filter traffic between different segments and block any unauthorized access.
2-5	Servers or data stores with sensitive information must be placed in dedicated separate network segments.
2-6	Firewalls and routers must be configured to prevent any unauthorized connections between untrusted networks and any system components storing confidential information.
2-7	Levels and boundaries must be defined and implemented for each security zone.
2-8	An out-of-band management network zone or segment, including all administration servers, machines with administrative access, Secure Shell (SSH) servers, jump servers and Privileged Access Workstations (PAWs), must be defined and implemented.
2-9	Wireless networks must be segregated from the internal network, isolated networks and private networks.
2-10	Servers, networks and production, test, and trusted environments used for developing, testing, scanning and storing data and any other related activities, must be clearly identified and segregated from other networks.
2-11	Segments of critical systems must be logically isolated from other environments.
2-12	Critical systems must be prevented from connecting to the wireless network.

2-13	Critical systems that offer internal services which do not require remote or Internet access must be prevented from connecting to the Internet
2-14	Security configurations, rules, policies and profiles for firewalls and routers that support critical networks must be reviewed at least every six months.
3	Boundary Defense
Objective	To protect the network boundary from cyber threats
Risk Implication	If the network boundary is left unprotected without the proper security controls, external attackers could easily breach the internal network and impose further serious threats.
Requirements	
3-1	An up-to-date inventory of all of <organization name>'s network boundaries must be maintained.
3-2	Regular scans from outside each trusted network boundary must be performed to detect any unauthorized connections that can be accessed across the boundary.
3-3	Communications with known malicious or unused Internet IP addresses must be denied, and access must be limited to trusted and necessary IP address ranges at each of <organization name>'s network boundaries.
3-4	Communication over unauthorized TCP or UDP ports or application traffic must be denied to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of <organization name>'s network boundaries.
3-5	Monitoring systems must be configured to record network packets passing through the boundary at each of <organization name>'s network boundaries.

3-6	Network-based Intrusion Detection Systems (IDS) sensors must be deployed to detect any unusual attack mechanisms and detect any compromise of these systems at each of <organization name>’s network boundaries.
3-7	Network-based Intrusion Detection and Prevention Systems (IDPS) must be deployed to block malicious network traffic at each of <organization name>’s network boundaries.
3-8	Network-based Advanced Persistent Threat (APT) detection/prevention systems must be deployed to detect or block malicious network attacks and zero-day attacks at each of <organization name>’s network boundaries.
3-9	Application inspection firewall must be deployed to block applications that are not whitelisted, unknown or non-compliant with security controls (for example, applications communicating over UDP/53 while not being compliant with DNS protocol) at each of <organization name>’s network boundaries.
3-10	Web Application Firewall (WAF) must be placed to analyses, filters, monitors, and blocks unauthorized Internet traffic to and from a web application.
3-11	Acceptable and approved encryption protocols such as some types of Transport Layer Security (TLS) must be configured to terminate on any WAF device to inspect decrypted traffic. If the device does not support TLS offloading, WAF must sit behind a decryption device to inspect decrypted traffic. Otherwise, a host-based web application firewall must be deployed.
3-12	The collection of NetFlow and logging data must be enabled on all network boundary devices.
3-13	All network traffic to/from the Internet must pass through an authenticated application layer proxy that is configured to filter unauthorized connections.

3-14	Only specific and whitelisted URL categories must be allowed to users. Access to hacking, malware, proxy, anonymizers, phishing, suspicious, unknown, and uncategorized URLs must be disabled.
3-15	All encrypted Internet browsing traffic at the boundary proxy must be decrypted prior to analysing the content. However, <organization name> may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.
3-16	All remote login access to <organization name>'s network must be configured to encrypt data in transit. Additionally, Multi-Factor Authentication must be used.
3-17	A remote access device that uses technologies such as Virtual Private Network (VPN), or SSL-VPN solutions must be deployed to terminate and protect all remote access to <organization name>'s network.
3-18	All devices remotely logging into <organization name>'s network must be scanned prior to accessing the network to ensure that all of <organization name>'s security policies have been enforced in the same manner used on local network devices.
3-19	Denial of Service (DoS) and Distributed DoS (DDoS) detection/prevention technologies must be deployed (on prim or by a third party) to detect or block DoS attacks at each of <organization name>'s network boundaries.
3-20	Domain Name System (DNS) security technologies must be deployed to detect and block DNS attacks at each of <organization name>'s network boundaries.
3-21	Domain Name System (DNS) query logging must be enabled to detect hostname lookups for known malicious domains.

3-22	Email security gateway must be deployed to detect and block email-based attacks at each of <organization name>’s network boundaries.
3-23	All subscription services, URL categories, threat feeds, blacklists, and signatures must be up-to-date and updated regularly.
4	Limitations and Controls
Objective	To minimize sources of attacks and protect the internal network from threats.
Risk Implication	Weak internal network and its associated constraints and controls increase the risk of internal threats and network lateral movement.
Requirements	
4-1	Active ports, services and protocols must be associated with the hardware assets in the asset inventory.
4-2	Only network ports, protocols, and services listening on a system with validated business needs must be running on each system.
4-3	Automated port scans must be performed on a regular basis against all systems, and alerts must be raised upon the detection of unauthorized ports on a system.
4-4	Host-based firewalls or port filtering tools must be applied on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
4-5	A datacenter firewall must be deployed to inspect and monitor inter-VLAN, trust-to-untrust, zone-to-zone, segment-to-segment, and east-west communications to protect the internal network and block internal attacks.

4-6	Firewall policies and rules model must be configured to follow positive security model (whitelisting model) by blocking all traffic by default and only allowing specific traffic to identified services. This can be achieved by configuring the last rule in an access control list to deny all traffic. In addition, this can be performed explicitly or implicitly, depending on the platform.
4-7	Datacenter firewall must be configured with application identification (Layer4-Layer7), and application whitelisting and blacklisting.
4-8	Firewall rules must be configured with user identification to build policies based on User identity (UID).
4-9	In case <organization name> network is IPv4 based, Layer 2 security controls must be deployed to protect the internal network.
4-10	Private/Isolated VLANs must be configured for critical network segments or isolated segments.
4-11	Networks or segments of critical systems must not be allowed to access any system in the environment unless they are scanned, and if required security controls are applied and security posture of the system is verified.
4-12	Communications network must be isolated by placing it in appropriate separate VLANs based on function and leveraging private VLANs or micro segmentation.
5	Wireless Access
Objective	To implement appropriate security controls for the use and protection of wireless networks.
Risk Implication	If the wireless network is left unprotected, <organization name> will be exposed to the risks of unauthorized connection to the network or data disclosure.

Requirements	
5-1	A comprehensive risk assessment exercise must be conducted to evaluate the risks of connecting wireless networks to the internal network.
5-2	An inventory of authorized wireless access points connected to the wired network must be maintained.
5-3	Network vulnerability scanning tools must be configured to detect and alert on unauthorized wireless access points connected to the wired network.
5-4	Wireless Intrusion Detection System (WIDS) must be used to detect/prevent and alert on unauthorized wireless access points connected to the wired network.
5-5	Wireless access on devices that do not have a business purpose for wireless access must be disabled.
5-6	Wireless access on client machines that do not have a business need for wireless access must be configured to allow access to authorized wireless networks only, and to restrict access to other wireless networks.
5-7	Peer-to-peer (ad hoc) wireless network capabilities must be disabled on wireless clients.
5-8	Wireless access points and wireless devices must be configured to connect to the wireless network using secure protocol such as WPA3.
5-9	Wireless networks must use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual Multi-Factor Authentication.
5-10	Wireless access of peripheral devices (such as Bluetooth and NFC) must be disabled unless such access is required for a business purpose.

5-11	A separate wireless network must be created for personal or untrusted devices. Enterprise access from this network must be treated as untrusted and must be filtered and audited accordingly.
6	Cryptography
Objective	To ensure the confidentiality of network data traffic and verify its confidentiality against unauthorized access and sensitive information disclosure.
Risk Implication	Lack of proper security technologies to ensure the encryption of network data may expose the <organization name>'s data to high cyber risks as a result of unauthorized access.
Requirements	
6-1	Network Cryptography must be implemented in accordance with <organization name>'s approved Cryptography standard.
6-2	The use of secure encrypted management protocols, such as Secure Shell (SSH) v2 and Remote Desktop Protocol (RDP) over TLS, must be enforced.
6-3	Sensitive and confidential network traffic must be encrypted by using next generation encryption cipher suites (such as Suite B cryptography) in accordance with <organization name>'s approved Cryptography standard.
6-4	Remote access traffic over IPsec or TLS must be encrypted with next generation encryption cipher suites (such as Suite B cryptography) in accordance with <organization name>'s approved Cryptography standard.
6-5	Application protocols must be configured to use encryption wherever applicable (HTTPS, FTP over SSL, LDAP over SSL, etc.)

7	Hardware and Software Integrity Validation
Objective	To ensure that all network software and hardware come from legal sources and that they have not been tampered with and verified .
Risk Implication	Intrusion in the supply chain is an opportunity to deploy and install malicious software and hardware within <organization name> network. Compromised software and hardware may affect the network's performance and jeopardize <organization name>’s data confidentiality, integrity and availability.
Requirements	
7-1	All physical network devices must be scanned for signs of tampering upon installation.
7-2	Software, updates, patches, and upgrades to network components must be obtained from validated sources.
7-3	When downloading software from the Internet, hash verification must be compared against the vendor’s database to detect unauthorized modification to firmware or software.
7-4	A change control process must be implemented and followed for any changes bearing a significant risk to <organization name>’s network, including rules that allow traffic to flow through network devices, firewall security policies, Network Address Translation (NAT), etc. The process must be documented and must include the following: • The rule’s purpose • The affected service(s) or application(s) • The affected users and devices • The date when the rule was added • The rule’s expiration date, if applicable • The name of the person who added the rule • The problem statement • Supporting data • Management’s approval of changes

8	Other Standard controls
Objective	To implement all network security standard controls and requirements to ensure the highest protection levels.
Risk Implication	Not applying the required security standard controls to protect the <organization name>'s network will expose it to cyber threats that disrupt operations and services.
Requirements	
8-1	The following standard controls must be implemented: 1- Disaster recovery and backup standard 2- Event and audit logging standard 3- Physical security standard 4- Wireless security standard 5- Secure and hardening configuration standard 6- National cryptographic standard controls

Roles and Responsibilities

1- **Standard Sponsor and Owner:** <head of the cybersecurity function>

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

3- **Standard Implementation and Execution:** <IT 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.