This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately.

Insert organization logo by clicking on the outlined image.

Wireless Network 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 cybersecurity requirements related to the protection of the security of the wireless networks of <organization name> to achieve the main objective which is minimizing cybersecurity risks resulting from internal and external threats at <organization name>.

The requirements in this standard 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 standard applies to all wireless network and systems of <organization name> and to all personnel at <organization name> (employees and contractors).

Standards

1	Wireless Network Segregation
Objective	To ensure the wireless network design and architecture are secure and the network segments are protected according to their security level.
Risk Implication	Networks without segregation share the same broadcast domain and are hence exposed to the same risks, 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	
1-1	A logically and/or physically segmented wireless network must be designed and implemented, taking into consideration

	business needs and enterprise architecture, and based on the principles of Defence-in-Depth and multi-tier architecture.
1-2	Appropriate level of security controls must be applied to different network segments based on the value and classification of information processed in the wireless network, levels of trust, business impact and associated risks.
1-3	Wireless networks must be designed and configured to filter traffic between different segments and block any unauthorized access.
1-4	Adjust firewall and routers settings to prevent any unauthorized connections between untrusted wireless networks.
1-5	Security configurations, rules, policies and profiles for firewalls and routers must be reviewed in regular bases in accordance to an approved plan.
1-6	Critical systems must be prevented from connecting to the wireless network.
2	Boundary Defence
Objective	To protect the wireless network boundary from threats.
Risk Implication	Poor network boundary protection without the proper security controls expose the networks to external attackers that could easily breach the internal network and impose further serious threats.
Requirements	
2-1	An up-to-date inventory of all of <organization name>'s wireless network boundaries must be maintained.
2-2	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 wireless network boundaries.
2-3	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 wireless network at each of <organization name>'s network boundaries.
2-4	Monitoring systems must be configured to record network packets passing through the boundary at each of <organization name>'s wireless network boundaries.
2-5	Network-based Intrusion Prevention Systems (IPS) must be deployed to block malicious network traffic at each of <organization name>'s wireless network boundaries.
2-6	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.
2-7	The collection of NetFlow and event logging must be enabled on all wireless network boundary devices.
2-8	All wireless network traffic to/from the Internet must pass through an authenticated application layer proxy that is configured to filter unauthorized connections.
2-9	Domain Name System (DNS) query logging must be enabled to detect hostname lookups for known malicious domains.
2-10	All subscription services, URL categories, threat feeds, blacklists, and signatures must be up-to-date and updated regularly.

3	Wireless Access
Objective	To control and protect the use of wireless networks.
Risk Implication	Poor protection of wireless network boundaries could expose <organization name> to the risks of unauthorized connection to the network or data disclosure.
Requirements	
3-1	A comprehensive risk assessment exercise must be conducted to evaluate the risks of connecting wireless networks to the internal network.
3-2	An inventory of authorized wireless access points connected to the wired network must be maintained.
3-3	Network vulnerability scanning tools must be configured to detect and alert on unauthorized wireless access points connected to the wired network.
3-4	Wireless Intrusion Detection System (WIDS) must be used to detect/prevent and alert on unauthorized wireless access points connected to the wired network.
3-5	Wireless access on devices that do not have a business purpose for wireless access must be disabled.
3-6	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.
3-7	Peer-to-peer (ad hoc) wireless network capabilities must be disabled on wireless clients.

3-8	Wireless access points and wireless devices must be configured to connect to the wireless network using secure protocol such as WPA3.
3-9	Wireless networks must use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual Multi-Factor Authentication.
3-10	Wireless access of peripheral devices (such as Bluetooth and NFC) must be disabled unless such access is required for a business purpose.
3-11	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.
3-12	Restrict transferring the classified data Top secret and Secret using wireless connection.
4	Hardware and Software Integrity Validation
Objective	To ensure and verify that all network hardware and software come from original sources and that they are not tampered with.
Risk Implication	Penetrations in supply chains allow the deployment of malicious software and hardware on <organization name>'s network. Compromised software and hardware may affect the network's performance and jeopardize <organization name>'s data confidentiality, integrity and availability. As a result, it will become possible to download unauthorized or malicious software onto the device after turned on.
Requirements	
4-1	All physical wireless network devices must be scanned for signs of tampering upon installation.

4-2	Software, updates, patches, and upgrades to wireless network components must be obtained from validated sources.
5	Other Standard controls
Objective	To implement all wireless network security standard controls and requirements to ensure the highest protection levels.
Risk Implication	Failure to implement all security standard controls and requirements exposes <organization name> to increased wireless network security risks.
Requirements	
5-1	The following standard controls must be implemented: 1- Backup and recovery standard 2- Event and audit logging standard 3- Physical security standard controls 4- Network security standard controls 5- Identity and access management standard controls 6- Secure and hardening configuration standard controls 7- Cryptography standard controls 8- Cybersecurity Incident and Threat Management standard controls

Roles and Responsibilities

1- **Standard 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.