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.

Mobile Devices 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 the detailed cybersecurity requirements related to Mobile Devices protection for <organization name> and Bring Your Own Device "BYOD" in order to minimize cyber risks resulting from internal and external threats at <organization name>.

The requirements in this standard are aligned with the Workstations, Mobile Devices, and BYOD Policy and 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 covers all Mobile Devices at <organization name> and all BYOD and applies to all personnel (employees and contractors) at <organization name>.

Standards

1	Device Access Locking
Objective	To ensure that unattended, lost and/or stolen devices cannot be accessed by unauthorized users.
Risk Implication	In case of unauthorized access to a mobile device owned by <organization name> and containing information pertaining to <organization name>, or if privileges are granted to access <organization name>'s IT environment, any potential work-related penetration could impact the department according to incident's severity.
Requirements	
1-1	Set up complex passcode configurations to be consisting of both upper-case letters, lower-case letters, numbers and special characters. Simple passcodes consisting of consecutive or sequential characters (e.g., 0000, 1234, 9876, etc.)must be

	prohibited. Passcodes consisting of additional character sets or greater lengths are recommended.
1-2	Whenever possible, additional authentication factor must be implemented to lock/unlock the mobile device (e.g., facial recognition, swiping pattern, fingerprint, One-Time-Password, etc.).
1-3	The passcode for the mobile device must be changed periodically or at least every three months.
1-4	Users must be prohibited from modifying or disabling security locking mechanisms.
1-5	The device auto-lock mechanism must be set to lock the device when it is idle and not being used for no more than 90 seconds or as per <organization name>'s requirements.
2	Device Contents Integrity
Objective	Apply a standard mechanism to prevent unintentional or harmful modifications to the contents of data stored on the device.
Risk Implication	If data stored on the device are tampered with, corrupted, or modified, neither the device nor stored data can be considered credible assets that may be used within <organization name>'s IT environment.
Requirements	
2-1	If the mobile device supports it, full device contents encryption must be enabled.
2-2	If supported by personal mobile devices (BYOD), data segregation between personal information and data owned by the <organization name> must be enabled and enforced. Additionally, segregated data must be encrypted.
2-3	BIOS bootloader passwords must be configured.
2-4	If the mobile device supports it, locking Bootloader must be enabled.

2-5	Encryption must be configured and enforced on any removable storage (e.g., SD cards or USB) that can be accessed by mobile devices.
2-6	The device must be set up to perform automatic lockout after five failed passcode entry attempts, and to perform data wiping after ten failed passcode entry attempts or as supported by the device operating system.
2-7	Wiping data remotely from lost/stolen devices must be enabled.
2-8	Modifying or disabling Bootloader locking by users must be prohibited.
2-9	Rooting or jailbreaking a mobile device must be prohibited, and the use of rooted or jailbroken devices within <organization name>'s IT environment must also be prohibited.
3	Device OS and Applications Security
Objective	To update and configure the operating system and applications installed on mobile devices properly prior to use.
Risk Implication	Installing unauthorized applications or failure to update operating systems and mobile devices' applications increases the likelihood of malware that could affect <organization name>'s IT environment.
Requirements	
3-1	Application installation must be allowed only from the organization approved applications or Vendor approved stores.
3-2	The permissions assigned to applications installed on a mobile device must be restricted, and the principle of Least Privilege must be applied.
3-3	Camera and Microphone must be disabled by default and access to them should be allowed based on need.

3-4	Application digital signatures must be verified before installation.
3-5	The mobile device must be updated to last Operating Systems (OS) versions/releases provided by the device vendor. If a device cannot be further updated to a newer OS, and the vendor has not provided security patches for the device in the last two years, the mobile device must be decommissioned and replaced.
3-6	Security Content Automation Protocol (SCAP) must be utilized to audit and verify all security configuration elements within the mobile devices, catalog approved exceptions, and report any unauthorized changes.
3-7	Users must not be able to modify or remove any secure configuration on the mobile device.
3-8	Disabling or removal of default accounts, and limiting access to accounts with high privilege based on identity and Access Management Policy.
3-9	A Minimum-Security Baseline for mobile devices must be developed, implemented and regularly monitored.
3-10	A regular full backup of data stored on the mobile devices must be performed as per <organization name>'s Backup Policy.
3-11	Mobile devices must be regularly patched and updated as per <organization name>'s Workstation and Mobile Device Security Policy and Patch Management Policy to ensure that all OS and application software is up-to-date.
3-12	Hardware controls must be implemented and access to removable media must be blocked where necessary or as per <organization name>'s Acceptable Use Policy.
3-13	Device control software must be implemented on all mobile devices to prevent unauthorized use of network communication tools (Wi-Fi, Bluetooth, etc.) or peripheral devices.

3-14	Disabling all information and file sharing features such s (Airdrop, NFC, and Bluetooth, etc.).
3-15	Protection software including antivirus, antimalware, application whitelisting and data leakage prevention software must be installed on all mobile devices.
3-16	Watermark feature must be used on users' screen.
3-17	Workstation secure configuration and hardening, including software and operating system level hardening, must be implemented in accordance with <organization name>'s Secure Configuration and Hardening Policy.
4	Other Standard controls
Objective	Implement all mobile devices 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 mobile devices security risks.
Requirements	
4-1	The following standard controls must be implemented: 1- Disaster recovery and backup standard 2- Event and audit logging standard 3- Malware protection standard 4- Cryptography standard 5- Secure and hardening configuration 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 function> & <cybersecurity 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 infrastructure, 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 Controls.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.