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.

Workstations, Mobile Devices and BYOD 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 use of workstations, mobile devices and privately owned devices (“Bring Your Own Device” BYOD) within <organization name> to minimize the cybersecurity risks resulting from internal and external threats 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 workstations, mobile devices and privately owned devices (“Bring Your Own Device” BYOD) used in <organization name>, as well as telework systems and it applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1- General Requirements

1-1 Data and information stored on workstations, mobile devices and BYOD must be protected as per their classification by the appropriate security controls to restrict access to such information and prevent access or viewing by unauthorized personnel.

1-2 Update workstations, mobile devices and BYOD software including operating systems, programs, and applications and implement the latest security patches must be according to the Patch Management Policy approved by <organization name>.

1-3 Implement secure configuration and hardening controls to workstations, mobile devices and BYOD must be in accordance with Cybersecurity Standards approved by <organization name>.

1-4 Personnel must not be granted privileged access to <organization name> systems using mobile devices and BYOD. Any access must be given following the Principle of Least Privilege.

1-5 Operating system and application default user accounts must be disabled or removed.

1-6 All workstations, mobile devices and BYOD must be centrally synchronized (Clock Synchronization) from an accurate and reliable source.

1-7 Workstations and mobile devices must be configured with an authorized use Banner.

1-8 Only whitelisted applications must be allowed on workstations and mobile devices.

1-9 Data Leakage Prevention must be used as well as data monitoring systems to ensure data protection on workstations and mobile devices.

1-10 Full Disk Encryption must be applied to privileged, advanced and critical systems access workstations and mobile devices storage media according to the <organization name> Cryptography Standard.

1-11 The use of external storage media must be restricted according to the <organization name>'s procedures after obtaining a prior permission from <Cybersecurity Function>.

1-12 Mobile devices and BYOD must be centrally managed by using Mobile Device Management (MDM).

1-13 Workstations, mobile devices and BYOD with end-of-life software including operating systems and application software must not be permitted to connect to <organization name>'s network to prevent security threats arising from unpatched end-of-life software.

1-14 Workstations, mobile devices and BYOD without up-to-date security software must be prevented from connecting to <organization name>'s network to avoid cyber threats causing unauthorized access,

malware infections or data exfiltration. Protection software include mandatory software such as Antivirus, Anti-malware, Host-Based Firewall and Host-Based Intrusion Detection/Prevention.

1-15 Deviations from acceptable user behaviour, risk assessment, and development and/or recommendation of appropriate countermeasures must be defined to mitigate them.

1-16 Unattended workstations and mobile devices must be configured to show a privacy screensaver protected with a password in case of Session Timeout for <5 minutes>.

1-17 Workstations and mobile devices accounts must be centrally managed through the Active Directory server of the <organization name>'s domain or Central Management System.

1-18 <Organization name>'s appropriate Group Policy must be enforced and applied on all workstations and mobile devices to ensure secure configuration and hardening and the organization compliance to regulatory and security controls, in addition to installing the necessary software.

1-19 A regular backup of data stored on workstations and mobile devices must be performed as per <organization name>'s Backup and Recovery Policy.

1-20 Techniques that allow the remote removal of data stored on mobile devices and BYOD must be provided and used under the following circumstances:

1-20-1 Mobile device is lost or stolen.

1-20-2 Upon end or termination of user employment at <organization name>.

1-20-3 Expiration of use and delivery of the mobile device to the concerned department <organization name>.

1-21 Telework systems and information devices must be protected through the following:

1-21-1 Implement Secure Session Management that includes session's authenticity, lockout, and timeout

1-21-2 Implement security patches on telework systems, at least once a month

1-21-3 Review telework systems protection configurations and hardening at least once a year.

1-21-4 Restrict enabling telework features and services on an as-needed basis, provided that potential cyber risks are assessed in case of need to enable them.

1-22 Awareness campaigns must be conducted on the safe ways to use mobile devices and BYOD as well as users' responsibilities in accordance with the Acceptable Use Policy approved by <organization name>, in addition to awareness campaigns dedicated to privileged access users.

1-23 Workstations, mobile devices and BYOD security procedures and criteria must be developed based on the work need.

1-24 Key performance indicators must be used to ensure the continuous improvement and proper and effective use of workstations, mobile devices and BYOD requirements.

2- Workstations Cybersecurity Requirements

2-1 Privileged access workstations must be dedicated to privileged technical team and must be isolated and connected to a dedicated Management Network without connection to any other network or service.

2-2 Privileged access workstations (PAWs) must be configured to forward logs to <organization name> central logging and monitoring system as per <organization name> Event Logs and Monitoring Management Policy and it cannot be reconfigured by user.

2-3 Workstations must be physically safeguarded within the buildings of <organization name> and facility entry/exit must be registered after

obtaining the necessary approvals as per <organization name> Physical Security Policy.

2-4 Protection of workstations from viruses, malware, advanced persistent threats (APTs), zero-day attacks and any other type of malicious attacks must be ensured through Endpoint Protection Software.

2-5 Integrity, availability and recoverability of workstation data must be ensured against tampering, accidental loss or damages.

2-6 All necessary security controls must be applied when removing workstations data, especially those connected to cloud services, as per <organization name> Data and Information Protection Policy.

2-7 Patches must be managed at least once a month for devices used to manage external and connected critical systems and at least once every three months for devices used to manage internal critical systems, as per <organization name>'s change management policy.

2-8 Configurations of devices used to manage critical systems must be reviewed and hardened at least once every six months.

3- Mobile Devices Cybersecurity Requirements

3-1 Mobile devices access to critical systems must be restricted only for a short period of time after conducting risk assessments and obtaining the necessary approvals from <cybersecurity function>.

3-2 It must be ensured that unattended, lost and/or stolen devices cannot be accessed by unauthorized users (Device Access Locking).

3-3 The integrity of information stored on mobile devices (Device Contents Integrity) must be ensured.

3-4 The operating system and applications installed on mobile devices must be properly updated and configured prior to use (Device OS and Applications Security) as per <organization name> technical standards.

3-5 Security patches for all mobile devices must be applied at least once a month.

3-6 Data and information of <organization name> stored on mobile devices must be encrypted and segregated.

4- BOYD Cybersecurity Requirements

4-1 In case workstations are used for business purposes, this must be supported by documented agreements with personnel along with technical security controls to protect <organization name> data and information.

4-2 Encrypt and segregate must be used for Data and information of <organization name> stored on mobile devices (BYOD).

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>

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

2- All personnel at <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.