BYOD POLICY

INLINE WITH ISO 27001, NIST AND SOC 2

PREPARED BY:

MINISTRY OF MOS SECURITY

BRING YOUR OWN DEVICE POLICY

CONTENTS

BRING YOUR OWN DEVICE POLICY

1. PURPOSE

This policy aims to define the rules for BYOD, or Bring Your Own Device, to determine when and how employees, contractors, and other authorized end users can use their own laptops, smartphones, and other personal devices on the <ORG NAME>'s network to access data and perform their job duties.

2. SCOPE

This policy applies to <ORG NAME> and all of their employees and contractors. This policy should be read in conjunction with the <ORG NAME>'s "Acceptable Usage Policy".

3. DEFINITION

Following is an explanation of various terms used within this document:

BYOD (Bring Your Own Device): Employees use their personal devices to connect to the <ORG NAME>'s network and access what they need to do their jobs.

Rooted device: Rooting is the process of unlocking or jailbreaking a device, such as a smartphone or tablet. It most commonly refers to Android devices.

Jailbroken device: Jailbreaking is the process of exploiting the flaws of a locked-down electronic device to install software other than what the manufacturer has made available for that device.

Registered device: When <ORG NAME>s want you to register the device, it means they can understand which devices are accessing secured resources, such as files and apps, and to possibly turn on conditional access to reduce the risk of inappropriate access to those resources.

BRING YOUR OWN DEVICE POLICY

4. RESPONSIBILITY

- The Chief Information security Officer (CISO) is responsible to review and approve the policy and ensure that it reflects the current requirements of Organisation.
- The Security & Compliance Office (SCO) is responsible for development, maintenance and enforcement of the policy.
- The SCO is responsible for conducting regular audits to ensure compliance to this policy.
- All employees and non-employees of Organisation are responsible to adhere to this policy in the course of their job duties.

5. GENERAL

The <ORG NAME> remains committed to enabling employees to do their jobs as efficiently as possible. This policy sets out requirements for employees to use personally-owned smartphones, tablets, desktops, and laptops to access the <ORG NAME>'s information, resources, and/or services.

All employees are allowed to access Office 365 via mails. An exceptional approval shall be taken by the CISO for using personal device like Laptop, Tablet, Desktops & removable media to access, store, process or transmit <ORG NAME> data.

The <ORG NAME> respects the privacy of the employee's personal device(s). The Security & Compliance Office (SCO) will only request access to the device if they believe that doing so is necessary to protect the <ORG NAME>'s interests. In those circumstances, The SCO may need to access employee's device to:

- Implement security controls or conduct audits
- Respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings
- Gather evidence during an investigation
- Investigate and remediate security breaches and other issues

This differs from <ORG NAME>'s policy for the equipment, software, and/or services we provide, where employees neither have the right nor should they expect privacy to the same extent while using its equipment, software, and/or services.

This policy is intended to protect the security and integrity of the <ORG NAME>'s data and technology infrastructure.

BRING YOUR OWN DEVICE POLICY

6. POLICY

BYOD-registered devices are subject to all of the <ORG NAME>'s information security-related policies and procedures. In particular, this policy is in addition to and should be read alongside the <ORG NAME>'s Acceptable Usage Policy.

6.1. Approval, registration, and support of devices

- The following devices are supported:
    - Mobile Devices - All models with up-to-date security patches available from the manufacturer.
    - Laptops - All models with up-to-date security patches available from the manufacturer.
      Note:

- For laptops, special approval is required from the Operations Head, CISO or SCO. Approval of usage of personal laptops for business activities will be subject to case-by-case analysis.
- No personal external storage devices are allowed to be used for business purposes.

6.2. Acceptable use of registered devices

- Acceptable business uses are those activities that directly or indirectly support the <ORG NAME>'s business.
- Acceptable personal use during the working day is limited to reasonable personal communication or recreation.
- At the <ORG NAME>'s discretion, employees will refrain from accessing certain categories of websites during work hours or while connected to the corporate network. Such website categories include, but are not limited to:
    - Adult and pornography websites,
    - Botnets,
    - Confirmed SPAM sources,
    - Gambling websites,
    - Keyloggers and monitoring websites,
    - Websites featuring illegal drugs or
    - Peer-to-peer downloading.

- Applications not downloaded through the official manufacturer App Stores (iTunes, Google Play, Microsoft Store) or from the official developer's website are prohibited.
- Devices must not be used at any time to:
    - Store or transmit illicit materials.
    - Store or transmit proprietary information.
    - Harass others.
    - Engage in outside business activities.

- Employees may use their mobile devices to access the <ORG NAME>'s assets, such as:
    - Email (through Outlook)
    - Calendars (through O365)
    - Contacts (through O365)
    - Documents through SharePoint/OneDrive

6.3. Security

- To prevent unauthorized access, registered devices must be password-protected by the guidelines defined in the <ORG NAME>s's "Password Management Policy" document.
- The registered device must lock itself with a password or PIN if it is idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden.
- Devices that are not on the company's list of registered devices are not permitted to be used.
- Employees are responsible for securing the information they access through their personal. Employees' access to <ORG NAME>'s information is automatically limited as set out in the <ORG NAME>'s "Access Control Policy" document.
- Employees must take all reasonable steps to prevent the theft or loss of registered devices.
- Employees are expected to maintain the registered device and ensure its systems are regularly updated and patched.
- Employees are expected to be aware of and comply with any regulatory or other requirements regarding handling personal data.
- Lost or stolen devices must be reported to the SCO as soon as is practical, and in every case, within 24 hours.
- Employees are responsible for notifying their mobile carrier immediately upon losing a registered device.
- A registered device may be remotely wiped if:

- The device is lost or stolen.
- The SCO detects a data or policy breach.
- The SCO detects a virus or similar threat to the security of the <ORG NAME>'s information or technology infrastructure.

6.4. Risks, Liabilities, and Disclaimers

- While IT services will take every precaution to prevent any personal data from being lost in the event that a registered device must be remotely wiped, all employees are responsible for taking additional precautions, such as backing up email, contacts, etc.
- <ORG NAME> reserves the right to disconnect registered devices or disable services in cases of a suspected threat or off-boarding of an employee.
- Employees are expected to use their registered devices ethically and adhere to "Acceptable Usage Policy".
- Employees are personally liable for all costs associated with their registered devices.

6.5. Breaches of the Policy

The <ORG NAME> will take all necessary measures to remedy any breach of this policy, including using <ORG NAME>'s disciplinary, legal, or contractual processes where appropriate.

7. Annexure A - Guidelines

7.1. Physical Security

- Mobile computing devices will be transported in a sturdy, waterproof, padded bag or compartment.
- Mobile computing devices will never be left unattended. It must be assured that they are secured anytime the employee is away from his or her desk.
- Mobile computing devices will not be placed near an open or unlocked window where they could be subject to theft.
- The mobile computing device's make, model, and serial number will be recorded in the asset inventory.

7.2. Data Security

- Mobile computing devices will be loaded with approved operating systems and have all relevant updates installed when available to ensure the security of the information residing on such devices.
- The operating system and application patch levels must be consistent with the current patch levels of the <ORG NAME> for similar devices and operating systems.
- All important data will be backed up and current copies will be kept readily available. Backup will be done on appropriate media.
- The storage will never be reformatted without prior testing of backed-up information.
- Unlicensed or pirated software will not be installed.
- All hard drives and USBs will be scanned for viruses, trojan horses, and other malware before use.
- Antivirus programs with the most recent updates will be installed as soon as they are available. The program will be configured for real-time protection, retrieve and install updates daily, and perform an antivirus or malware scan at least weekly.
- Additional malware protection software must be active on mobile computing devices in accordance with the Antivirus Policy.

7.3. When Traveling

- Care will be taken not to forget or misplace the mobile device while traveling.
- The mobile device will not be kept unattended, even during a security check at an airport.
- The mobile device will not be checked in with baggage.
- When traveling out of the country, proper documentation must be carried out to ensure easy passage.

7.4. Network Security

- Employees will meet the following requirements when connecting their mobile devices to a network:
    - Determine whether the antivirus program is up-to-date, has the latest virus definitions, appropriately configured, and runs correctly. If one of these conditions fails or the mobile device has not been scanned for viruses within the last week, a full virus scan must be conducted before the device can be used on any network.
    - Test the mobile devices and scan for additional malware through tools such as adware or spyware tests to determine whether the device has a worm.

- Test the state of stored sensitive data to ensure it is protected.
- Remove any malware on the mobile device, if detected. Information about any malware found must be logged and reported to the CISO.
- If the mobile computing device is owned by an outside <ORG NAME>, the <ORG NAME> must agree in writing to allow antivirus and malware scans of their devices.

8. POLICY REVIEW AND MAINTENANCE

- This policy shall be reviewed at least annually or in response to significant changes in technology, business operations, or regulatory requirements.
- Changes must be approved by senior management and communicated to stakeholders.

9. TRAINING AND AWARENESS

- All employees shall undergo training on the guidelines of this policy as part of onboarding.
- Regular refresher training on defined practices shall be conducted.
- Employees must acknowledge compliance with this policy at least annually.

10. ENFORCEMENT

10.1. Policy Violations

Violation of the policy will result in corrective action from the management. Disciplinary action will be consistent with the severity of the incident, as determined by the investigation, and may include, but not limited to

- Loss of access privileges to information assets
- Termination of employment or contract
- Other actions deemed appropriate by management, HR division, Legal division and their relevant policies

BRING YOUR OWN DEVICE POLICY

Violation or deviation of the policy shall be reported to the Security & Compliance Office and a security incident record has to be created for the further investigation of the incident.

10.2. Policy Exceptions

Any exception to this policy has to be formally approved by the Chief Information Security Officer. All the exceptions shall be formally documented in the standard IT exceptions request form.

The exception request shall follow the below mentioned approval matrix.

First level	Unit Manager/Reporting Manager
Second Level	Chief Information Security Officer

DID YOU FIND THIS DOCUMENT USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

WWW.MINISTRYOFSECURITY.CO