INSERT LOGO

BRING YOUR OWN DEVICE POLICY (BYOD)

Classification: Internal

This document may only be shared internally without prior confirmation from the owner.

Version	Approved By	Owner	Date Last Updated	Review Frequency	Next Review	Comments

Contents

Purpose of the Policy

[Company Name] recognises employees' desire to use personal devices. This policy defines the security standards for such devices and the user's responsibilities.

INSERT LOGO

Scope

This policy covers:

- Anyone who uses their personal device for [COMPANY NAME] business purposes.
- Devices handling [COMPANY NAME] data, such as;
  - Mobile phones
  - Computers (Laptops / Desktops, etc)
  - Tablets / Electronic notepads
  - USBs

Responsibilities

Line Managers will;

- Oversee team compliance.

All employees must;

- Follow this policy & procedures.
- Inform their manager or IT of any policy violations.

IT Team will;

- Aid in the policy's execution.

Exceptions

- Exceptions should be requested via the IT Help Desk.

Device Security

- Users must protect their devices against unauthorised access. Secure measures include;
  - Passwords (see the password policy)
  - PIN codes
  - Biometrics (facial or fingerprint)

Minimum Device Requirements

- Devices must run the latest operating system and have updated security patches. IT will enforce access via 'conditional access rules'. For clarification, contact the IT Help Desk.
- Install antivirus and anti-malware software.
- Set devices to update security patches automatically.
- Encrypt devices. For assistance, consult the Helpdesk.

Data Storage

- Avoid storing company data on personal clouds or unencrypted drives.
- Refrain from saving sensitive information about employees or [COMPANY NAME] contacts on personal devices.
- Never store signatory reports and evaluations on personal devices.

Remote Device Management

- [Company Name] retains the right to oversee and control BYOD devices, especially for security and data/applications related to [Company Name].

Incident Reporting

- Report any security issues concerning BYOD devices to the IT team immediately.

Costs

- Employees bear all device and operating costs.

Termination of Employment

- On employment termination, staff must erase [Company Name] data and passwords from their devices. Relevant details should be passed to their manager.

Training Requirements

- New employees receive this policy and must familiarise themselves with it.