Mobile Device Policy

Pronounced80 Solutions Limited

Freeing business from the tyranny of legacy software

Version 1.0 | Effective: May 2026 | Review: Annual

1. Purpose

To ensure mobile devices used for business purposes are configured securely.

2. Scope

Laptops, tablets and smartphones used to access company or client systems and data.

3. Mandatory Controls

- Device encryption (FileVault / BitLocker / native mobile encryption).
- Strong passcode / biometric unlock.
- Automatic screen lock (≤ 5 minutes idle).
- Operating system and applications kept up to date.
- Endpoint protection where applicable to device type.
- Approved app sources only (App Store / Play Store / vendor sites).
- Find My Device / remote wipe capability enabled where supported.

4. Authentication

- Unique account; MFA enabled for email, identity, source control and cloud admin where supported.

5. Data Handling

- Client confidential data accessed only via approved apps/services.
- No client data stored in personal cloud accounts.

6. Lost or Stolen Devices

- Reported to the Director immediately.
- Remote sign-out and credential rotation actioned promptly.
- Remote wipe initiated where appropriate.

7. Disposal

- Devices wiped/factory reset and verified before disposal, sale or recycle.

8. Travel

- Devices kept in personal possession or secured.
- Avoid unsecured public Wi-Fi for client work; use VPN where required.