MOBILE / BYOD / POLICY

Mobile Device and BYOD Policy

A small-business policy for company phones, personal phones used for work, lost devices, MFA apps, and basic mobile security expectations.

Purpose

This policy sets expectations for mobile devices used to access company email, files, applications, messaging, customer data, or business systems.

The goal is to protect company data while allowing practical mobile work.

Scope

This policy applies to company-owned phones and tablets, personal devices used for work, and any mobile device used for multi-factor authentication, business communication, file access, or customer support.

Device access requirements

Any mobile device used for company work must:

- Use a passcode, PIN, password, biometric unlock, or equivalent screen lock
- Lock automatically after a short period of inactivity
- Run a supported operating system version
- Receive security updates
- Avoid jailbreaking, rooting, or bypassing built-in security controls
- Use encrypted storage where supported by the device
- Be reported promptly if lost, stolen, replaced, or transferred to another person

Company-owned devices

Company-owned devices are business assets. The company may manage, configure, restrict, update, wipe, replace, or inspect them as needed to protect business operations and data.

Employees should not use company-owned devices for activities that increase risk, including unauthorized apps, illegal content, unsafe downloads, or storing personal sensitive information that would interfere with business management of the device.

Personal devices used for work

Personal devices may be used for work only when approved by the company. Approval may depend on role, data access, customer requirements, and technical controls available for the device.

The company may require security settings on personal devices that access company data, including screen lock, managed email profiles, device compliance checks, application controls, or remote removal of company data.

The company should avoid accessing personal photos, personal messages, personal browsing history, and non-work personal files unless required by law or a specific investigation.

Work data on mobile devices

Employees should access company data through approved apps and accounts. Company files should not be copied into personal cloud storage, personal email, personal messaging apps, or unapproved note-taking tools.

Screenshots of customer records, regulated data, internal systems, passwords, or security alerts should be avoided unless required for support and stored in an approved location.

Messaging and communication

Employees should use approved company communication tools for business conversations. Sensitive business decisions, customer records, regulated data, credentials, or incident details should not be handled through personal text messages or consumer messaging apps unless specifically approved.

MFA and authenticator apps

Mobile devices used for MFA must be protected with a strong unlock method. Employees must report lost or replaced phones promptly so MFA methods can be removed or re-enrolled.

Employees must not approve MFA prompts they did not initiate. Unexpected MFA prompts should be reported as a possible account compromise.

Public Wi-Fi and travel

When using public Wi-Fi, employees should avoid accessing sensitive company systems unless using approved protections such as VPN, trusted cloud applications, or secure remote access tools.

Employees should be especially careful in airports, hotels, conferences, hospitals, government offices, and shared workspaces.

Lost, stolen, or replaced devices

Employees must report lost or stolen devices as soon as possible. The report should include:

- Device type
- Phone number or asset tag if known
- Last known location
- Whether the device had company email or files
- Whether the device was used for MFA

The company may remove company data, revoke sessions, reset passwords, disable MFA methods, or take other steps to reduce risk.

Device disposal and transfer

Before a device is sold, traded in, recycled, transferred, or given to another person, company accounts and data must be removed. Company-owned devices must be returned or processed according to company instructions.

Enforcement

Devices that do not meet this policy may be blocked from company systems. Policy violations may result in access removal, retraining, disciplinary action, or other appropriate measures.

Implementation checklist

- Require screen lock on all devices used for work
- Require MFA for business accounts
- Document approved mobile apps
- Create a lost-phone reporting process
- Remove old phones from MFA enrollment
- Decide whether BYOD is allowed for each role
- Use mobile device management where risk justifies it

Disclaimer

This starter policy is general information, not legal advice. Adapt it to your business, contracts, regulatory obligations, and state law.