

BYOD and Mobile Device Policy

Purpose

Workforce members increasingly use personal phones, tablets, and laptops, and company-issued mobile devices, to reach Your Organization data from many places. This policy sets the conditions that keep company data protected on those devices while respecting the personal data of their owners.

Scope

This policy applies to all workforce members, including employees, contractors, and temporary staff, who access Your Organization email, files, applications, or networks from a device that Your Organization does not fully manage (personal devices, "BYOD") or from a company-issued mobile device. It applies to smartphones, tablets, laptops, and wearables that can store or display company data.

Roles and responsibilities

- **The IT team** operates the mobile device management (MDM) or equivalent service, maintains enrollment, and performs remote actions.
- **The security team** owns the minimum security baseline and approves exceptions.
- **Device owners** keep their devices updated, enrolled, and in their own control, and report loss promptly.
- **Managers** decide whether a role needs mobile access to company data.

Requirements

1. Eligibility and enrollment

- Access to company data from a personal device is a privilege granted by the manager and the IT team, not a right, and may be withdrawn at any time.
- A device must be enrolled in Your Organization's MDM or app-protection service before it can reach company email, files, or applications. Unenrolled devices are blocked by conditional access where technically possible.
- Devices that are rooted, jailbroken, or running an operating system version that no longer receives security updates are not permitted.

2. Minimum security baseline

Every device that accesses company data must:

- Use a screen lock with a PIN, password, or biometric, and auto-lock after no more than five minutes of inactivity.
- Have device storage encryption enabled.

- Run a supported operating system with security updates applied within 30 days of release, and sooner for actively exploited vulnerabilities.
- Install apps only from the official app store of the platform.
- Use multi-factor authentication for company accounts.
- Run endpoint protection where the platform supports it.

3. Protection of company data

- Company data is accessed through managed or approved applications. Where possible, Your Organization uses app-level containers so that company data can be removed without touching personal data.
- Company data is not copied to personal cloud storage, personal email, or unapproved messaging apps.
- Confidential data is not stored locally on personal devices unless it is within the managed container.
- Company data is not displayed or discussed in public where others can see or overhear it.

4. Remote access

- Access to internal systems from any device uses Your Organization-approved VPN or zero-trust access.
- Public or shared computers (for example, hotel or library kiosks) must not be used to sign in to company systems.
- Connections over untrusted wireless networks go through the approved VPN or an equivalent protected channel.

5. Lost, stolen, or compromised devices

- A lost or stolen device, or a device suspected of compromise, is reported to IT and security within 24 hours, even if the device was personal.
- Your Organization may remotely lock the device, remove the managed container, or in the case of a company-owned device wipe it fully. For a personal device, Your Organization limits remote actions to company data and managed apps wherever the platform allows.
- Reported incidents are handled under the Incident Response Plan.

6. Privacy of the device owner

- Your Organization does not read personal messages, photos, or personal app data on a personal device and limits the information it collects to what the MDM service needs: device model, operating system, compliance state, and the list of managed apps.
- The data collected and its use are described in the enrollment notice, which the owner acknowledges before enrollment.

7. Offboarding and device changes

- When a workforce member leaves, or replaces or disposes of a device, company data and managed apps are removed and the device is unenrolled. Access is removed under the Access Control Policy.
- Company-issued devices are returned and are sanitized under the Media Protection Policy.

8. Cost and support

Your Organization does not guarantee support for personal devices. Any stipend or reimbursement is set by separate HR policy.

Exceptions

Exceptions require written approval from the security team, a description of the compensating controls, and an expiry date.

Enforcement

Non-compliant devices may be blocked or have company data removed. Violations by individuals may lead to disciplinary action in line with the Acceptable Use Policy.

Evidence

Evidence of operation includes the MDM enrollment and compliance report, conditional access rules, acknowledged enrollment notices, and records of remote lock and wipe actions.

Review cadence

This policy is reviewed annually by the security team and IT, or sooner when mobile platforms, tooling, or laws on employee device monitoring change.

Effective date: [the date this policy takes effect]