

Mobile Device Management Policy Template

A free, fill-in-the-blank policy for company-owned phones, tablets, and laptops: ten sections, a device register, a lost-device checklist, and a framework mapping guide.

Company: _____ Effective date: _____

Policy owner: _____ Review cycle: At least annually, and after any change to device model or tooling

HOW TO USE THIS TEMPLATE

Replace every [bracketed field] with your own details, delete the guidance notes, then have leadership approve and date the final document. Sample times are illustrative starting points, not benchmarks. This policy covers company-owned devices. Personal devices belong in a separate BYOD policy. This template is a starting point, not legal advice. See ComplyJet's [Mobile Device Management Policy guide](#) for the reasoning behind each section.

1. Purpose and Scope

This policy defines how [Company] issues, enrolls, configures, secures, recovers, and retires company-owned devices, so that every device has a named user and every stage leaves auditable evidence.

It applies to all employees, contractors, and temporary staff who use a company-owned phone, tablet, or laptop, and to every such device regardless of where it is used. It does not cover personally owned devices, which are governed by the [BYOD Policy].

2. Roles and Responsibilities

Role	Responsibility
Policy Owner ([IT Lead])	Maintains this policy, the Device Register, and the device management tool. Approves exceptions.
Device User	Keeps the device secure, reports loss or theft within the stated deadline, and returns the device on request or at exit.
HR / People Operations	Triggers device return and access removal as part of every offboarding.
Leadership	Approves this policy and any standing exceptions.

3. Eligibility and Issuance

Company devices are issued from the approved list of [models] based on role. Each device is recorded in the Device Register at issuance (see the register layout below) before it is handed to the user.

4. Enrollment

All company-owned devices must be enrolled in [device management solution] before they are issued. An unenrolled device may not be used to access company systems or data. Users must not remove management profiles, disable security software, or jailbreak or root a device.

5. Security Requirements

Control	Requirement
Disk encryption	Full-disk encryption is enabled and enforced on every laptop and phone.
Screen lock	Automatic lock after [5] minutes of inactivity, protected by a passcode that meets the [Password Policy].
Operating system updates	Security updates applied within [14] days of release. Unsupported versions are blocked from company systems.
Endpoint protection	Installed, running, and reporting on every device where the operating system supports it.
Password manager	Required for work credentials. Saving credentials in browsers or notes is not permitted.
Remote lock and wipe	Enabled and tested before the device is issued.

6. App Management and Acceptable Use

Apps may be installed only from [approved app stores]. The following categories are blocked: [list]. Company data must be accessed only through managed or approved apps. Devices must not be shared with family or friends, and company data must not be stored in personal cloud accounts. General acceptable use rules are set out in the [Acceptable Use Policy].

7. Lost, Stolen, and Remote Wipe

A user who loses a company device, or suspects theft, must report it to [IT Lead] within [1 hour] of discovery. The Policy Owner will lock and locate the device, revoke the user's sessions and credentials, and record the incident. If the device is not recovered within [24 hours], or held regulated data, a full remote wipe is performed and the event is assessed as a possible data breach under the [Incident Response Plan].

GUIDANCE

State which wipe your tooling actually performs: full device, or corporate account only. Do not promise a full wipe the configured tier cannot deliver.

8. Employee Privacy

Device management collects device state: model, operating system version, encryption and lock status, and app inventory. It does not collect message content, photos, or browsing history. Location is used only to recover a lost or stolen device, and each use is logged. Personal accounts and files should be kept on personal devices; company devices may be inspected for security reasons. Administrator access to the management console is limited and reviewed.

User acknowledgment: I have read and understand Section 8. Name: _____ Date: _____

9. Offboarding and Return

1. The device is returned by [last working day + 5 days], with shipping arranged for remote staff.
2. Company account access is removed and all sessions are signed out on the last working day.
3. The device is wiped and unenrolled on return, and the date is recorded.
4. The device is reissued after a clean wipe, or sanitized for disposal under the [Media Disposal Procedure].
5. The Device Register is updated and the record retained for audit history.

10. Exceptions, Review, and Enforcement

A device that cannot meet this policy may be used only under a written exception stating the reason, compensating controls, an expiry date not longer than [12] months, and approval by [Leadership role]. The Policy Owner reviews this policy at least annually. Violations are handled under [disciplinary / HR security policy].

Device Register Layout

Serial no.	Model	Assigned user	Issue date	Enrolled	Encrypted	Status

Lost or Stolen Device Checklist

Step	Done by / time
☐ Report received and logged	
☐ Device locked and location checked	
☐ Sessions, tokens, and credentials revoked	
☐ Recovery deadline passed or regulated data involved: full wipe issued	
☐ Breach assessment completed and documented	
☐ Device Register updated	

Framework Mapping Guide

Framework	Where it applies	What it expects	Sections above
SOC 2	CC6.1, CC6.7, CC6.8	Logical access controls, restricted movement and removal of information, prevention and detection of unauthorized or malicious software	4, 5, 6, 7
ISO 27001:2022	Annex A 8.1 (also 5.11, 6.7, 7.9)	Protection of information on user endpoint devices, return of assets, remote working, assets off-premises	3, 4, 5, 9
HIPAA	45 CFR 164.310(d)(1), 164.312(a)(2)(iv)	Controls over hardware and media containing ePHI; mechanism to encrypt ePHI (addressable)	5, 7, 9
GDPR	Articles 32 and 33	Appropriate technical security measures; breach notification where personal data is exposed	5, 7
PCI DSS 4.0	Requirements 1.5.1, 12.2.1	Security controls on computing devices connecting to the cardholder data environment; documented acceptable use of end-user technologies	5, 6