Document Name: [COMPANY] Mobile Device Management Policy
Last Revision: [INSERT]
Next Revision: [INSERT]
Document Owner: [INSERT TEAM(S)]

# [COMPANY] Mobile Device Management Policy

Version 1.0

**CONFIDENTIAL**

# Table of Contents

# Introduction

At [COMPANY], we recognize the importance of mobile devices in enabling our employees to work efficiently and stay connected. This Mobile Device Management (MDM) Policy provides guidelines for using company-owned and personally-owned mobile devices (Bring Your Own Device - BYOD) that access company data or systems. The goal is to ensure the security of our business while allowing employees the flexibility to use mobile technology in their work.

# Objectives

The purpose of this policy is to:

- Protect [COMPANY] data and systems from unauthorized access or data breaches resulting from the use of mobile devices.
- Provide clear guidelines for securing both company-owned and personal devices that connect to company resources.
- Ensure compliance with data privacy regulations and security best practices.
- Outline employee responsibilities and acceptable use of mobile devices.
- Minimize the risk of data loss in case of lost, stolen, or compromised devices.

# Scope

This policy applies to:

- All employees, contractors, vendors, and third parties using mobile devices to access [COMPANY] data, systems, or networks.
- All mobile devices, including smartphones, tablets, and laptops, whether they are company-owned or personally-owned (BYOD).
- Both on-site and remote use of mobile devices.

# Device Eligibility

- **Company-Owned Devices:** Employees may be issued company-owned mobile devices (e.g., smartphones, tablets) for business use. These devices are pre-configured with [COMPANY] security settings and monitored under this policy.
- **BYOD (Bring Your Own Device):** Employees may use personal mobile devices for work purposes, provided they comply with [COMPANY] security requirements and are approved by the IT team.
- **Device Approval:** Before any personal or company-owned device can access [COMPANY] resources, it must be approved and registered with the IT team.

# Security Requirements for Mobile Devices

To protect company data, all mobile devices used for business purposes must meet the following security requirements:

- **Encryption:** All company data stored on mobile devices must be encrypted to protect against unauthorized access.
- **Password Protection:** Devices must be secured with a strong password, PIN, or biometric authentication (e.g., fingerprint, facial recognition). Passwords must meet the company's password policy (see Password Management Policy).
- **Remote Wipe:** In the event that a device is lost or stolen, the IT team must be able to remotely wipe company data from the device. Employees must agree to this capability as a condition of using their personal device for work.
- **Automatic Lock:** Devices must automatically lock after a period of inactivity (no longer than 5 minutes).
- **Software Updates:** Employees are responsible for ensuring their devices are regularly updated with the latest security patches and operating system updates.
- **Mobile Device Management (MDM) Software:** [COMPANY] may require MDM software to be installed on mobile devices to manage security settings, monitor device compliance, and enforce policies remotely.
- **Antivirus and Anti-Malware Software:** Devices accessing company systems must have antivirus or anti-malware software installed and kept up-to-date.

# Acceptable Use of Company Mobile Devices

- **Work-Related Activities:** Mobile devices should be primarily used for work-related activities, including accessing company email, systems, and applications.
- **Personal Use:** Limited personal use of mobile devices is permitted, provided it does not interfere with work responsibilities, violate company policies, or introduce security risks.
- **Data Access:** Employees must avoid accessing sensitive company data over public or unsecured Wi-Fi networks. A VPN (Virtual Private Network) must be used for secure access to company systems when working remotely.
- **App Installation:** Only company-approved applications should be installed on devices that access [COMPANY] data. Employees must not install unauthorized or untrusted apps that may pose a security risk.
- **Data Backup:** Company data accessed or stored on mobile devices must be regularly backed up according to company guidelines to prevent data loss.

# Monitoring and Enforcement

To ensure compliance with this policy, [COMPANY] reserves the right to monitor mobile devices used to access company resources. Monitoring may include, but is not limited to:

- MDM Software Monitoring: MDM software may be used to track device compliance with security policies, detect unauthorized access, and enforce security settings.
- Usage Logs: [COMPANY] may log and review mobile device access to company systems, including the use of company data, applications, and networks.
- Remote Access Management: If a device is found to be non-compliant or poses a security risk, the IT team may remotely lock or wipe company data from the device to protect [COMPANY] assets.

Monitoring will be conducted in accordance with applicable privacy laws, and employees will be notified of any major changes to monitoring practices.

# Lost or Stolen Devices

In the event that a mobile device used for company purposes is lost, stolen, or otherwise compromised, the employee must:

- Report Immediately: Notify the IT team within 24 hours of discovering the loss or theft of the device.
- Remote Wipe Activation: Authorize the IT team to remotely wipe any company data from the device to prevent unauthorized access.
- Password Changes: Change any company account passwords that were used on the device as soon as possible.

The IT team will review the incident and take appropriate measures to mitigate any risks to company data or systems.

# Appendix A: Revision History

This is a controlled document. This section highlights major and minor changes to the document as it is revised.

| Revision | Date | Description | Approved by |
|---|---|---|---|
| 1.0 | | Initial Version | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |