Here's a sample **Mobile Device Use Policy** that you can adapt for your organization. This version is suitable for small to mid-sized businesses but can be customized based on your specific industry or needs.

Mobile Device Use Policy

Effective Date: [Insert Date]
Last Updated: [Insert Date]

1. Purpose

This policy outlines the acceptable use of mobile devices to protect the security and integrity of [Company Name]'s data and network, whether devices are company-owned or personally owned (BYOD – Bring Your Own Device).

2. Scope

This policy applies to all employees, contractors, and temporary workers who use mobile devices (e.g., smartphones, tablets, laptops) to access company systems, data, or communication tools.

3. Acceptable Use

Employees may use mobile devices for:

- Accessing work email, calendars, and business applications.
- Communicating with coworkers, clients, and stakeholders.
- Remote work and travel-related activities.

Limited personal use is permitted, provided it:

- Does not interfere with work performance.
- Does not consume excessive network or IT resources.
- Adheres to the company's code of conduct.

Mobile devices may NOT be used while driving. The exceptions are;

- While using a hands-free device.
- For company business only.

4. Security Requirements

All mobile devices accessing company resources must:

- Use a strong password, PIN, or biometric lock.
- Enable device encryption and automatic locking.
- Have up-to-date antivirus and OS/security patches.
- Allow remote wipe capabilities in case of loss or theft.

5. Prohibited Activities

The following activities are strictly prohibited:

- Downloading or installing unauthorized apps or software.
- Storing sensitive company data unencrypted.
- Jailbreaking or rooting a device.
- Using the device to harass or bully others.
- Accessing or transmitting illegal, offensive, or inappropriate content.

6. Reporting and Compliance

Employees must immediately report:

- Lost, stolen, or compromised devices.
- Suspected data breaches or unauthorized access.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.

7. Company Rights

[Company Name] reserves the right to:

- Monitor mobile device usage related to company data or systems.
- Revoke access at any time.
- Wipe corporate data from devices when an employee leaves or if the device is compromised.

8. BYOD Specifics (If Applicable)

Employees using personal devices must:

- Agree to a Mobile Device Agreement.
- Allow installation of management tools (e.g., MDM) as required.
- Understand that company data may be wiped remotely if needed.

9. Acknowledgment

All users must sign the Mobile Device Use Agreement acknowledging they understand and will comply with this policy.

Disclaimer
The recommendations contained in this Loss Control document are provided solely for informational purposes. They are not intended to constitute legal, safety, or engineering advice, nor do they guarantee compliance with any local, state, or federal regulations. Implementation of these recommendations is at the discretion of the client and should be evaluated in the context of their specific operations, risk tolerance, and applicable laws.
Neither the author nor the issuing organization assumes any liability for damages or losses that may result from the use or misuse of this information. It is the responsibility of the client to consult with qualified professionals as needed to ensure appropriate risk management and regulatory compliance.