**Sample Mobile Device Security Policy**

*By Michael Goad*

*Use the following template as an example when building a mobile device security policy. Requirements and management practices vary between organizations, so administrators should modify the policy according to their organization's business needs and update it as needed.*

**1.0 Purpose**

This policy outlines the rules for using mobile devices to access business data, whether they are company-owned or personal devices. Employees are allowed to use their personal smartphones and other mobile devices for work purposes, as it is convenient for them. However, if an employee does not follow the procedures and policies outlined in this policy, <company name> reserves the right to revoke the privilege of using personal devices at work and for work-related activities.

**2.0 Scope**

This policy covers any mobile device that can access or store company data. This includes but is not limited to corporate or personally-owned laptops/notebooks, tablets, mobile phones and smartphones.

**3.0 Policy**

**3.1. Acceptable Use**

When using their devices to interact with corporate data or connect to the corporate network, employees must comply with the following guidelines:

* Users must always keep their apps up to date when accessing work content and resources.
* The mobile device should have basic protections, such as passcodes, and encryption must be enabled.
* Employees should not access websites and content deemed to be illicit, proprietary or illegal.
* Employees should not use their devices for work-related tasks during activities such as driving or operating machinery or hosting and sharing content in the corporate network.

**3.2. Device Restrictions and Security**

Users must comply with the following protective measures when using mobile devices:

* Employees must keep their devices updated with the latest firmware and operating systems. Additionally, they must use the antivirus software that <company name> provides on their mobile devices.
* Employees must create passwords that meet the company's minimum character requirement for their devices.
* Employees are prohibited from installing illegal or pirated software on any mobile device that is used to access company data.
* Users should not store any business information that has not been encrypted using approved encryption methods.
* Data should be stored in approved tools and applications.
* Authorized users must take reasonable precautions to prevent mobile devices from being stolen or accessed without permission.
* Report any loss, theft or security incident related to a mobile device to IT immediately.

The following sections specify business requirements for data security as they relate to specific types of mobile devices.

**3.2.1. Laptops (Windows and macOS)**

All company‐owned or issued laptops accessing corporate systems must enable the following security measures:

* Management by company MDM or other management system.
* Encryption.
* Username and Password policy enforcement and/or biometrics.
* Updates of the device's OS based on OS compliance policies.
* Installation and maintenance of security tools, including antivirus, that <company name> provides.
	+ Users must not disable any security controls or interfere with automatic updates or security patches provided by <company name>.

**3.2.2. Smartphones and Tablets**

To access corporate systems and data from smartphones and tablets, users must enroll those devices in the company-approved and managed MDM, <MDM platform name>. This MDM platform requires a device PIN/password, contains a company-issued certificate and enforces two-factor authentication for security purposes. By agreeing to the terms of the MDM platform, users grant <company name> permission to perform a remote wipe if the device is lost or stolen. Users must enroll in <MDM platform name> to access company email and applications.

To ensure the security of the system, smartphones and tablets must be updated to the latest operating system and security patches within designated timeframes. Devices that do not meet the minimum requirements will be prevented from synchronizing email and accessing company data and applications.

**3.3. Audits**

<Company name> may conduct periodic audits of devices to ensure compliance with the requirements of this policy.

**3.4.** **Use and Return of Mobile Devices**

**3****.4.1. Issuance Record for Company-Owned Mobile Devices**

<Company name> will maintain a record of all users who receive corporate-owned mobile devices. It is the responsibility of the user to ensure that they comply with the policy requirements, which includes taking necessary steps to prevent theft or unauthorized access to the device, enrolling the device into the company management system and keeping the device compliant with the company policy. If a user no longer requires the device or is leaving the company, it is their responsibility to return all corporate-owned mobile devices.

**3.4.2. Removal of device data**

Before reissuing a mobile device, <company name> will remove all confidential information stored on the device in compliance with company policy.

**4.0 Enforcement**

Possible consequences of noncompliance with the mobile security policies include:

* + Removal of corporate data.
	+ Device quarantine.
	+ Remote wipe and reset.

<Company name> may also take disciplinary action against the noncompliant user, ranging from suspension of technology privileges to termination of employment, based on the user's noncompliant actions.