

Example Mobile Device Security Policy

Using this policy

One of the challenges facing IT departments today is securing both privately owned and corporate mobile devices, such as smartphones and tablet computers. This example policy is intended to act as a guideline for organizations looking to implement or update their mobile device security policy.

Feel free to adapt this policy to suit your organization. Where required, adjust, remove or add information according to your needs and your attitude to risk. This is not a comprehensive policy but rather a pragmatic template intended to serve as the basis for your own policy.

Background to this policy

The most common challenge is that users do not recognize that mobile devices represent a threat to IT and data security. As a result they often do not apply the same security and data protection guidelines as they would on other devices such as desktop computers.

The second challenge is that when users provide their own devices they often give greater weight to their own rights on the device than to their employer's need to protect data.

This outline policy gives a framework for securing mobile devices and should be linked to other policies which support your organization's posture on IT and data security.

Example policy

1. Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals.

However mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

<Company X> has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

2. Scope

1. All mobile devices, whether owned by <Company X> or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers.
2. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted being authorized by security management.

3. Policy

3.1 Technical Requirements

1. Devices must use the following Operating Systems: Android 2.2 or later, IOS 4.x or later. <add or remove as necessary>
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with <Company X>'s password policy. This password must not be the same as any other credentials used within the organization.
4. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

3.2 User Requirements

1. Users must only load data essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to <Company X> IT immediately.
3. If a user suspects that unauthorized access to company data has taken place via a mobile device they user must report the incident in alignment with <Company X>'s incident handling process
4. Devices must not be "jailbroken"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact <Company X> IT.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.
9. Devices must be encrypted in line with <Company X>'s compliance standards.
10. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify <Company X> IT immediately.
11. (If applicable to your organization) Users must not use corporate workstations to backup or synchronise device content such as media files unless such content is required for legitimate business purposes.

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.