SOPHOS
Security made simple.

Sample 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 who need to implement or update an existing mobile device security policy.

Feel free to adapt this policy to suit your organization's risk tolerance and user profile. Where required, adjust, remove or add information to customize the policy to meet your organization's needs. 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

Corporate IT departments face two challenges when contemplating a BYOD policy: a mix of corporate and employee owned devices accessing the organization's network and data, and the use of those devices for both professional and personal purposes.

With data flowing across public networks, to and from devices that are easily lost or stolen, protecting data becomes a paramount concern and the primary driving force for implementing Mobile Device Management systems and policies. Security must be central to an organization's workforce mobility strategy in order to protect corporate data, maintain compliance, mitigate risk and ensure mobile security across all devices.

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.

As a Bring Your Own Device program can only be successfully implemented if certain security policies are enforced, we would expect a Mobile Device Management solution to be a prerequisite for this policy.

Sample policy

1. Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and <CompanyX> supports their use to achieve business goals.

However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized 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 and applications.

2. Scope

1. All mobile devices, whether owned by <Company X> or owned by employees, inclusive of smartphones and tablet computers, that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops.
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 authorized by security management must be conducted.
3. Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

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. Only devices managed by IT will be allowed to connect directly to the internal corporate network.
5. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

3.2 User Requirements

1. Users may only load corporate data that is 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 must report the incident in alignment with <Company X>'s incident handling process.
4. Devices must not be "jailbroken" or "rooted"* 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 untrusted 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 may 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. The above requirements will be checked regularly and should a device be non-compliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
12. The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to a non compliant device being wiped for security reasons.
13. (If applicable to your organization) Users must not use corporate workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

*To jailbreak/root 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 unauthorized software.

3.3 Actions which may result in a full or partial wipe of the device, or other interaction by IT

1. A device is jailbroken/rooted
2. A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user)
3. A device is lost or stolen
4. A user has exceeded the maximum number of failed password attempts

3.4 Use of particular applications which have access to corporate data

1. Cloud storage solutions: Company X supports the use of the following cloud storage solutions xxxxxx
2. The use of solutions other than the above will lead to a compliance breach and the loss of access to the corporate network for the user

Try Sophos Mobile Control

BYOD is today's reality. If you embrace these devices, you'll see the productivity gains, efficiencies, and innovations they bring to a mobile workforce. But you must have the right solutions in place from the start.

We invite you to try Sophos Mobile Control for free. See how easy and cost-effective it can be to secure your end users, their mobile and web access, and your business data. And our per user licensing means that you can say yes to BYOD without limiting the number or the type of devices your end users carry. Take control of mobile security with Sophos Mobile Control.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK