NOTIFY TECHNOLOGY

WHITEPAPER

SAMPLE BYOD MOBILE DEVICE SECURITY POLICY

A guide to help organizations define technical requirements, user responsibilities, and compliance scenarios.

Notify Technology Corporation

888 Boardman-Canfield Rd, Ste C
Boardman, OH 44512

(234) 228-7100 | sales@notifycorp.com

www.notifycorp.com

Using this Policy

One of the challenges facing company IT departments today is securing privately owned smartphones and tablets. This example policy is intended to act as a guideline for organizations who need to implement a BYOD policy for mobile devices

Feel free to adapt this policy to suit your organization's risk tolerance and user profile. This is not a comprehensive policy but rather a pragmatic template intended to serve as the basis for your own policy.

Background to this BYOD Policy

A good BYOD policy has two characteristics: (1) Policies are clearly defined, and (2) they are enforced. A BYOD policy should cover the following items:

- Address acceptable use, security controls and the rights of the company to secure and manage the employee-owned device. .
- Explain that the mobile management application will be required for an employee to use their personal device to access company resources.
- Clarify that the mobile management application will create a separate "work" and "personal" segmentation of their device.
- Explain that the security and management oversight will only apply to the company information found in the "work" side of their device. No oversight or privacy breeches of privacy will occur on the "personal" side of their mobile device.

This outline of a BYOD 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. A Bring Your Own Device program can only be successfully implemented if certain security policies are enforced, we recommend Notify's MobileRMM™ platform as the mobile management solution to be a prerequisite for this policy.

Sample BYOD Policy

Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the Company and supports their use to achieve increased productivity and business goals.

Supporting a BYOD practice certainly has some potential benefits, but it also can create potential legal, compliance, and support challenges. BYOD security is often a challenge for a company. This stems from the fact that to be effective, companies must exert some form of control over smartphones and tablets that are not owned by the company but are employees' personal assets.

This document outlines a BYOD policy that defines a set of practices and requirements for the safe use of iOS and Android mobile devices.

Scope

The scope of this BYOD policy only includes employee-owned iOS and Android smartphones and tablets and is focused on the "work" segment of the personal mobile device. The company will limit the scope of its management and security of the employee's personal mobile device to those threats that create a legal and compliance issue on the "work segment" portion of the device.

The company will not manage or violate any privacy issues regarding the following items of the end user's mobile device.

- Personal email accounts
- Personal pictures and videos
- Personal non-work-related applications
- Personal Files
- Personal Music

BYOD Policy

Technical Requirements

All employee-owned devices will be enrolled in the Company's mobile management solution whereby the following requirements will be implemented and enforced.

- Personal devices should be running the latest available version of iOS and Android operating systems.
- Upon enrollment into a mobile management platform, a user's device will be partitioned into a "personal" and "work" side and only the "work" side will be managed by the Company.
- All enrolled devices will be subject to the valid compliance rules on security features such as encryption and passcode as well as rooted/jailbreak detection.
- Only devices enrolled using the Company's mobile management platform will be allowed to connect directly to the company network.
- All enrolled devices will have company email and applications installed and configured on the "work" side of their mobile device.

User Responsibilities

- Users must report all lost or stolen devices to company management immediately.
- If a user suspects that unauthorized access or use of their mobile device, they must report the incident to the appropriate Company manager.
- Devices must not be "jailbroken" or "rooted". [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.]
- It is recommended that applications installed on the "personal" side of their device come from trusted sources.
- Devices must be kept up to date with manufacturer or network provided OS updates.
- It is recommended that users must be cautious about opening links from text messages as well as links in emails where the sender is not a known entity.

Compliance Scenarios

- Scenarios which may result in a full or partial wipe of the device, or other interaction by IT include:
  - ✓ Their mobile device is jailbroken/rooted
  - ✓ Their mobile device contains an app known to contain a security vulnerability (if not removed within a given timeframe after informing the user)
  - ✓ Their mobile device is lost or stolen
  - ✓ A user has exceeded the maximum number of failed password attempts
  - ✓ A user has resigned or been terminated

About Notify

Notify is a highly experienced ISV focused on delivering a mobile management platform to MSPs and IT services providers. Notify's MobileRMM™ offers a security and management solution for both BYOD and company owned iOS and Android devices. Notify's Partner Program provides all the essential support elements needed by an MSP or IT service providers to offer a mobile managed service to its customers.

For more information about Notify's MobileRMM™ and Partner Program, email **sales@notifycorp.com** or call **(234) 228-7100**.

Notify Technology Corporation

888 Boardman-Canfield Rd, Ste C
Boardman, OH 44512

(234) 228-7100 | sales@notifycorp.com

www.notifycorp.com