This is a sample mobile device policy meant to be used as part of an employee handbook. The purpose of this document is only to provide a sample guideline and a framework for generating a mobile device policy for your clients' use. This sample can be customized for use as an overall Mobile Device Policy or a Bring Your Own Device (BYOD) Policy.

<Company> Mobile Device (BYOD) Policy

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 (personal or company owned) also represent a significant risk to company information security and data protection. 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 costly data leakages and system infection.

<Company> developed this mobile device policy to protect our information assets in order to safeguard our customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of all mobile devices when accessing the corporate network and is intended to protect the security and integrity of <Company's> data and technology infrastructure. <Company> reserves the right to restrict the use of mobile devices if users do not abide by the policies and procedures outlined below.

Scope

All mobile devices, whether owned by <Company> 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. Limited exceptions to the policy may occur where there is a business need; however, a risk assessment must be conducted by management and written approval provided in advance.

In order to connect mobile devices to the company network, employees must agree to the terms and conditions set forth in this policy, and install required software onto their mobile devices.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of <Company>.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Employees are blocked from accessing certain websites during work hours or while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to: <list of restricted websites>
- Mobile devices' cameras and video capabilities <are / are not> disabled while on-site.
- Mobile devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities
- The following apps are allowed: <list allowed apps>
- The following apps are not allowed:
  - Any apps not downloaded through iTunes or Google Play
  - <list additional restricted apps>

- Employees may use their personal mobile device to access the following company-owned resources: email, calendars, contacts, documents, <list additional resources>
- <Company> has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Mobile Devices and Support

- Mobile devices must use the following operating systems: Android 2.0 or later or Apple iOS 3.1 or later.
- Connectivity issues are supported by IT; however, employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Mobile devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network. This includes the installation of mobile device management (MDM) software on all mobile devices that access the company network.
- <Company> will support the following mobile device features utilizing the MDM software:
    - Configure access to corporate Exchange email accounts
    - Configure access to personal email accounts
    - Configure virtual private network (VPN) settings
    - Configure Wi-Fi network settings
    - Enable access to the corporate directory for use in composing emails
- <Company> will not utilize the MDM software to:
    - Track an employee's current location or previous locations unless attempting to locate a lost or stolen device (lost devices will only be traced upon approval of the device owner)
    - Access an employee's personal or corporate emails, text messages or other messages
    - Access contact information or other information stored on the device (personal or company)
    - Access social networking or other applications installed on the device

Security

- In order to prevent unauthorized access, mobile devices must be password protected using the features of the device.
- Passwords must contain a minimum number of characters. Passwords will be rotated every 90 days and the new password may not be one of 15 previous passwords. Password must not be the same as any other credentials used within the organization.
- The mobile device must lock itself with a password or PIN if it is idle for five minutes.
- After five failed login attempts, the device will autowipe.
- Rooted (Android) or jailbroken (iOS) mobile devices are strictly forbidden from accessing the company network.
- Employees are prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.
- Users must not load pirated software or illegal content onto their mobile devices.
- Users must not store company data of any kind in unapproved applications on the mobile device.
- Mobile 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 one time per month.

- Mobile devices must not be connected to a PC or a laptop which does not have up-to-date and enabled anti-malware protection and which does not company with corporate policy.
- Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the company network.
- Users may not use corporate workstations to backup or synchronize mobile device content such as media files unless such content is required for legitimate business purposes.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's mobile device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- In the event IT must remote wipe a device, all data on the mobile device will be lost, including personal data. It is the employee's responsibility to take additional precautions, such as backing up email, contacts, photographs, media files, etc.
- The company reserves the right to disconnect mobile devices or disable services without notification.
- Lost or stolen mobile devices must be reported to the company immediately. Employees are responsible for notifying their mobile carrier upon loss of a personal mobile device.
- If an employee suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident to the company immediately.
- The employee is expected to use his or her mobile devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her mobile device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the mobile device unusable.
- <Company> reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

Mobile Device (BYOD) Policy Acceptance Form

I have read and understand the foregoing mobile device (BYOD) and acceptable use policy and agree to adhere to the policies set forth. I agree to have mobile device management software installed on my mobile device and understand that the data on my mobile device may be erased and the device returned to factory settings if lost or stolen or if my employment is terminated, resulting in a loss of the corporate and personal information stored on the device. I understand that backing up the information stored on my mobile device is my responsibility.

_____

Employee Signature Date

_____

Printed Name

Sources:
Berry, Megan. IT Manager Daily. BYOD Policy Template. http://www.itmanagerdaily.com/byod-policy-template/
Sophos. Example Mobile Device Security Policy.