Sample BYOD Policy

This document provides policies, standards, and rules of behavior for the use of personally-owned smart phones and/or tablets by <Department Name> employees to access <Department Name> resources and/or services. Access to and continued use is granted on condition that each user reads, signs, respects, and follows the <Department Name>'s policies concerning the use of these resources and/or services.

This policy is intended to protect the security and integrity of <Department Name>'s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Expectation of Privacy

<Department Name> will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for <Department Name> provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using equipment and/or services.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of <Department Name>.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Devices may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information
  - Harass others
  - Engage in outside business activities
  - Etc.
- Employees may use their mobile device to access the following company-owned resources:
  - Email
  - Calendars
  - Contacts
  - Documents
  - Etc.
- <Department Name> has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and Support

- The following devices are supported:
  - iPhone (3GS, 4, 4S, 5, etc…)
  - iPad (<list acceptable models>)
  - Android (<list acceptable models>)
  - Blackberry (<list acceptable models>)
  - Windows (<list acceptable models>)
  - Etc…
- Connectivity issues are supported by IT; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.
- 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.

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.
- The company's strong password policy is: Passwords must be at least six characters and a combination of upper- and lower-case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can't be one of 15 previous passwords.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The employee's device may be remotely wiped if:
  - The device is lost or stolen.
  - The employee terminates his or her employment.
  - 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

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, but it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The company reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her 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 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 device unusable.
- <Department Name> reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of <Department Name> services. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device is not provided.

Employee Name: ____

BYOD Device(s): ____

Employee Signature: ______________________________ Date: __________