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.