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.