# Mobile Device Policy

Company grants its employees the privilege of utilizing their self-purchased smartphones and tablets of for their convenience for work related purposes.

Company reserves the right to revoke this privilege if users who do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of Company’s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Company employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

## Definitions

**Company data** - All electronically stored

* client confidential information
* confidential organizational, financial, and personnel information
* non-confidential information owned by Company

**Mobile Device** - Any device that is or may be used to access or store Company data while the device is outside of the offices of Company including devices that are not the property of Company but are used to access or store Company Data.

**Company Computer** - Any Personal Computer (laptop or stationary PC) that is the property of Company and is a mobile device and any Notebook Computer that is the property of Company.

**Private Computer** - Any Personal Computer or Notebook Computer that is not the property of Company.

## Scope

This policy applies to any Mobile Devices that accesses or stores Company Data.

## Acceptable Use

Company defines acceptable business use as activities that directly or indirectly support the business of Company.

Company defines acceptable personal use on company time as reasonable and limited personal communication or recreation during breaks.

Employees are blocked from accessing certain websites while connected to the corporate network at the discretion of Company.

Devices may not be used at any time to:

* Store or transmit illicit materials
* Store private client data unless this data is encrypted using Company-approved methods.
* Store or transmit proprietary information belonging to another company
* Harass others
* Engage in outside business activities

Employees may use their mobile device to access the following Company-owned resources: email, calendars, contacts, documents.

Company has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

## Devices and Support

Allowed tablets include iPad running iOS version 6 or above, Android-based tablets running version 4 or above, and Windows 8 tablets.

Connectivity issues are supported by IT for networks at Company locations; employees should contact the device manufacturer or their carrier for operating system or hardware-related or cellphone data network 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.

## Reimbursement

Company will not reimburse the employee for the cost of the device.

Company will not pay the employee an allowance or cover the cost of any part of the phone or data plan.

## 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. Mobile device passwords must be a minimum of 4 characters.

Company’s password policy is: Passwords must be at least eight characters and must be 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 5 previous passwords.

The device must lock itself with a password or PIN if it’s idle for five (5) minutes.

After five failed login attempts, the device will lock. Contact IT to regain access.

Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

Storage is encrypted.

The lock screen will provide owner contact information should the device be lost.

Employees are not automatically prevented from downloading, installing and using any app that does not appear on Company’s list of approved apps, but may be asked to remove apps that have the potential for creating a risk for which Company would become liable.

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
* employment is terminated
* IT detects a data or policy breach, a virus or similar threat to the security of Company’s data and technology infrastructure.

## Apps

To the extent that Company data is stored in apps other than those provided or hosted by Company, usernames and passwords must be provided to IT and the app must be listed on the Approved App List before it may be used for Company purposes. A Company-provided email address must be used when setting-up accounts for these apps and their related services.

## 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, it is the employee’s responsibility to take additional precautions, such as backing up any personal information on the device.

Company reserves the right to disconnect devices or disable services without notification.

Lost or stolen devices must be reported to 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 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.

Company reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.