BYOD Policy

The Company grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. The Company reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.
This policy is intended to protect the security and integrity of The Companies data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.
The 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.

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of The 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/while connected to the corporate network at the discretion of the company.
- Devices' camera and/or video capabilities are/are not disabled while on-site.
- 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
  - Etc.
  - Check your Approved App list with IT department
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- The Company has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed
- Tablets including iPad and Android are allowed
- Connectivity issues are supported by IT; employees should/should not 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.

- Backup of data will be the responsibility of the employee, but where work related data needs to be secured it must be stored in the correct network locations to ensure that it complies with the current back up processes of the Company.

Reimbursement

- The company will not reimburse the employee for the cost of the device
- The company will not reimburse the employee for the cost of the applications installed on the device, but will supply the work related software to the employee free of charge.

Security

- All devices that allow for Domain Authentication needs to JOIN the Microsoft Windows Domain, of the Company (Discuss with the IT department)
- All Logon Policies need to be run on the device as prescribed by the Logon notice.
- Users will not be allowed to have Local administration rights on the device while logging onto the domain as per Domain policies.
- 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. This will be set by a Policy on the network.
- The device must lock itself with a password or PIN if it's idle for more than 5 (five) minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.
- Smartphones and tablets belonging to employees that are for personal use only are/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 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

- 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 personal data, 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.
- The employee assumes full liability for any software licensing on the device for Software not supplied by The Company for business use.
- The Company reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.