**ELECTRONIC DEVICES POLICY - BRING YOUR OWN DEVICE**

Use of personal electronic devices, including but not limited to smartphones, tablets, laptops and computers, for work purposes is allowed only when management has provided written authorization and may be limited to certain employees or departments.

During working hours and while conducting company business, employees must exercise the same discretion in using their personal devices as is expected for the use of company devices. All company policies in effect pertaining to harassment, discrimination, retaliation, proprietary information, trade secrets, confidential information and ethics apply to the use of personal devices for and during work-related activities.

Nonexempt, hourly employees will generally not be authorized to use their personal devices for work purposes. In the event that an hourly employee receives management authorization to use personal devices, the employee may not use their device for work purposes outside of their normal work schedule without authorization in advance from management. This includes but is not limited to reading, sending and/or responding to work related e-mails, text messages, or phone calls (answering and initiating). Hourly employees will be paid in accordance with federal and state law for all hours worked.

Employees may not use their personal devices for work purposes during periods of unpaid leave without prior management authorization. The Company reserves the right to deactivate the Company’s information and access on the employee’s personal device during periods of unpaid leave.

To ensure the security of proprietary company information and technology, employees who have been authorized by management to use personal devices are required to comply with Company requirements regarding the installation of anti-virus software, additional encryption software and “remote-wipe” software by the IT department. All company-related information and applications must be stored in a way that is password-protected and secure. Cloud-based applications or backup software programs may not be used unless authorized specifically by management, as these programs may allow company-related information to be transferred to unsecure parties. Additionally, employees may not use unsecure internet connections.

Employees using devices that have camera, video or recording technology are restricted from using those capabilities anywhere on company property at any time unless authorized, in writing, in advance, by management.

When personal devices are being used for work purposes, employees should not expect any privacy except that which is governed by law. The Company has the right, at any time, to monitor any communications that utilize the Company’s networks in any way, including data, voicemail, telephone logs, Internet use, network traffic, etc., to determine proper use. The Company reserves the right to review, retain, monitor or release personal and/or company-related data on personal devices to government agencies or third parties during an investigation or litigation. The Company may review the activity and analyze usage patterns and may choose to publicize these data to assure that the Company’s resources in these areas are being utilized according to this policy. Finally, no employee shall knowingly disable, tamper with, alter or destroy any network software or system identified as a monitoring application.

Employees are expected to reasonably protect personal devices used for work-related purposes from loss, damage and theft. If a personal device is lost or stolen, the employee must notify the Company immediately. The Company may choose to remotely wipe company-related data. The Company is not responsible for the loss or damage of other data and applications on the device when it is remotely wiped. The Company bears no responsibility for replacing or repairing personal devices that are damaged even if that damage occurs on Company property and/or during working hours.

The employee may be asked to produce any personal devise used for work purposes at any time for inspection or review of compliance with policy. When an employee resigns or is terminated, the employee must cooperate in allowing access to the personal device so that the IT Department can remove all company data.

Failure to follow these policies and procedures may result in disciplinary action up to and including termination of employment.