HUMAN RESOURCES POLICY

SUBJECT:	**Personal Electronic Devices at Work (PED)**	**NO:**
DEPARTMENT:		**ISSUED BY:**
ISSUE DATE:		**REVISION DATE:**

The company allows employees to use their personal electronic devices for work purposes provided they comply with the following requirements. This policy applies to all employees.

Federal and/or State laws require that certain information must be kept confidential. This includes all employee medical and personal information. Our company also requires that employees protect both employee and business information. This includes all pricing information, customer/client information, marketing plans, financial information, and other business data. Employees, including those who use a personal electronic device, such as a laptop, Smartphone, tablet, or other personal electronic device with the capacity to store information, must first obtain permission to capture and store company information. Once approval is obtained from management, it is imperative to protect the device(s) from loss or unauthorized access by any other person. All employees must review and accept the company confidentiality/privacy policies and procedures. It is a condition of employment.

These precautions must be taken by all employees with PEDs.

- Password protect every device
- Make certain all data is encrypted
- Establish a pass phrase
- Use only secure wireless networks
- Establish a 10 minute "Time Out" limit with re-access only with the password
- Make certain the make, model and serial number is recorded in case of theft
- Establish a two-step authentication process for copying
- If it is available, download and use the mobile application (app) that assists in finding a missing PED

If you need assistance to protect your PED, please see
and notify immediately if your PED is lost or stolen.

All company data captured or stored on a PED is company property and may only be used for company-related work. If the employee abuses the information, terminates employment, or changes devices, the company may remotely wipe the information from the device. All data must be uploaded to the company server once each week on .
Any information/data stored on an employee device will be treated as any other physical property the company owns. It may never be stored using any unapproved third-party software or transferred to a non-approved device. This includes using any software that has been labeled as a "*data security risk*." Do not download information to a flash drive that can easily be lost or stolen.

All company files and documents stored on an employee device must be returned at the time of separation of employment or upon request. Failure to comply will be treated in the same way the company treats theft of any other company property. The company will seek the appropriate legal remedy when there is an unauthorized breach of security of the information or the information/data is not returned to the company *and* subsequently deleted from the

device(s). Employees, who use a personal data device as part of their work, should have no expectation of privacy. The company may access the device at any time. Although it is not the intent of the company to review or to store any employee personal information on the company server, unless there is appropriate segregation of information, it may not be possible to avoid accessing non-business information and privacy is not guaranteed. The company reserves the right to require the employee to use specialized software for business purposes to avoid co-mingling company and personal information.

The company forbids any employee from capturing and storing personal or private employee information on a personal electronic device. This includes storing employee name, address, phone number, date of birth, race, gender, or social security number, in a single data file. These are the major employee identifiers. When they are stored in a single file, they provide opportunities for abuse by identity thieves. Storing a contact list (name and phone number) is acceptable. Maintaining employee personal medical information on a personal device is prohibited because of the restrictions under HIPAA.

Non-exempt employees (those who receive overtime pay) may not conduct company work on a personal device outside regular work hours, unless that work has been authorized and the time is properly recorded. Non-exempt employees may not respond to work emails, voice mails, or texts regarding work, unless authorized by management, as this may be described as working overtime without being compensated.

If you have any questions regarding this policy, please contact .

Approved by:	**Title:**	**Date:**