BRING YOUR OWN DEVICE (BYOD)

This policy provides guidelines for using personally owned devices and related software for business use.

The BYOD policy applies to all Earnhardt employees, contractors, vendors and any other person using or accessing Earnhardt information or information systems. Exceptions to this policy must be approved by the IT Director or a designated representative.

Earnhardt management reserves the right to determine which employees can use personally owned devices based on the amount of personally identifiable information (PII) with which an employee works.

General Policy

Earnhardt recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by Earnhardt for corporate use:

- Tablets
- Personal digital assistants (PDAs)
- Smart phones

Registering Devices

All personally owned devices must be password protected and registered with the Earnhardt IT department.

End-user Support

As a general rule, users of personally owned devices will not use or request corporate IT resources in the use, network connectivity or installation of their equipment or software. With the exception of access to any Earnhardt systems, users are responsible for learning, administering, installing and setting up their personally owned devices.

Device Security

The user must follow good security practices, including:

- Password protect all personally owned devices.
- Do not leave personally owned devices unattended.

Release of Liability and Disclaimer to Users

Employees hereby acknowledge that the use of personally owned devices in connection with Earnhardt business carries specific risks for which the employee, as the end user, assumes full liability.

In the case of litigation, Earnhardt may take and confiscate a user's personally owned device at any time.

Acceptable Use

The Electronic Communications System Policy in The Earnhardt Employee Manual applies to personally owned devices.

Authorization of Devices

Earnhardt IT reserves the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access.

Third-party Applications on Devices

Earnhardt IT reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

As the number of approved applications continually evolves, the user must check with the IT department for the current list of approved third-party applications and get IT approval before downloading it to the device.

Remote Wiping

Even though Earnhardt does not own the device, it does own all company data. Earnhardt reserves the right to remotely wipe the user's personally owned device at any time. The goal of the remote wiping process will be to clean the device of the company data; however, the user's personal data also will be at risk. The user accepts the risk of the loss of personal data and acknowledges that Earnhardt shall have no liability for the loss of any such personal data.

Reporting Security Concerns

The user agrees to report the following immediately:

- If the device is lost or stolen.
- If the device has been attacked by malware, a virus or any other suspicious attack.

ACCEPTED AND ACKNOWLEDGED:

____
(Signature)

____
(Print Name)

____
(Date)