BYOD Agreement

Certain employees of CEO will have the opportunity to use their personal electronic device(s) for work purposes ("Users"). User's use of their personal electronic device(s) for work purposes must be authorized in writing, in advance, by management. Such access is a privilege that may be revoked by CEO at any time.

It is important that Users understand the scope of permissible use of their personal mobile devices and the Employer's rights with regard to these devices. Therefore, each User must read, understand, and comply with this agreement. This will help minimize the risk, both to the User and CEO, inherent in the abuse or misuse of these devices.

All wireless/mobile devices, including, but not limited to, laptops, smart phones (iPhone®, Android®, etc.), and tablets (iPad®, Galaxy®, Nexus®, etc.) and any other Employer-supported device that accesses the Employer's information system (collectively "Device"), are subject to the Employer's security and system/configuration requirements.

No Device may be connected to the CEO's s information system unless it has been approved, configured, and registered. In so doing, **the User consents to allow the Employer to install software, updates, manage configuration settings, and make any and all necessary adjustments to the Device to support connectivity to and security of the Employer's information system**. The **User also consents to the Employer's access to any applications containing CEO data stored on any Device if that Device is or ever has been used to connect to the Employer's information system**. **The User further consents to the Employer wiping the Device of any Employer information and data.**

Security of Your Device.
The following guidelines must be followed:

- Passwords. Each User is required to have a password on their Device.

- Suspicious activity. If a User becomes aware of any type of suspicious behavior associated with the Device such as a virus or other type of malware, the User is expected to contact the Employer immediately. In some cases, it may be necessary to wipe and reset the Device to resolve such issues.

- Avoiding theft. All Devices are targets for theft. Each User is responsible for protecting their Device and must not leave it unattended in public places.

9573001.2 5/25/2022

- Forwarding data or email files to another personal account or device. Employees who are using a personal device may not forward or copy any files or agency data to a non-agency or personal account.

- Ownership of email messages and Data files. CEO retains ownership of the content of any messages, such messages and data are the sole property of CEO regardless of the form and/or content of these messages and data.

- Privacy. You are expressly advised that in order to prevent misuse, Employer reserves the right to monitor, intercept, review, and remotely wipe, without further notice, all Employer content on your device. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings, and your privacy related such personal data is protected in accordance with applicable law.

- Investigations and Litigation. In the event of an investigation, litigation, or other legitimate business reasons, CEO reserves the right to review and/or retain Employer-related data on a Device or to release the data to government agencies or third parties. Accordingly, Users should have no expectation of privacy with regard to Devices utilized to access the Employer's information system.

Use of Mobile Devices

- Working Time. Mobile devices are tools available to assist Users with communication via email, phone, and computer (laptop) and voice mail during working time. The Employer prohibits non-exempt employees from accessing, responding to, or using these devices for work-related purposes outside of normal working hours. If, in the rare instance, a non-exempt employee needs to use a Device to conduct Employer business outside their normal work schedule, the employee must obtain prior authorization from their supervisor and notify their supervisor of their time worked to insure they will be properly compensated.

- Use by Third Parties. To safeguard confidential information that may be stored thereon, passwords to access applications containing CEO information or otherwise used for work purposes may not be shared or used by other individuals.

- Compliance with Policy. When using Devices, whether Employer-issued or personal, Users are required to comply with CEO's policies concerning technology, confidentiality, discrimination, harassment and retaliation as well as other applicable policies.

- Adherence to Law. All Users are to adhere to applicable law and safe practices when using such Devices.

Loss of Your Device

- If a Device is lost or stolen, the User is expected to **immediately notify the IT Administrator to** disable/wipe the Device. Disabling the Device will prevent someone

9573001.2 5/25/2022

from accessing confidential information contained on it and prevent inadvertent access to the CEO's information system.

Applications

- CEO has the right to delete any application on the Device if such application creates a problem with access to the network or a security breach. IT may need to wipe and reconfigure the Device to resolve an issue with an application that is on a Device.

I understand that I have been approved to utilize a personal device for business purposes and will comply with all provisions outlined in this policy.

By signing, I acknowledge that I have read and agree to the above.

User's Name: _____

Signature:_____

Date:_____

9573001.2 5/25/2022