BRING YOUR OWN DEVICE TO WORK POLICY

The Organization permits [SPECIFIED EMPLOYEES] to use their own personal electronic devices, including but not limited to smartphones, tablets, and laptops, computers, mobile phones, and cellphones ("**devices**"), to perform work for the Organization or on the Organization's behalf. However, to protect the Organization and its employees, any use of a device for business purposes must conform to this policy as described below. In addition, each user is responsible for using their device in a sensible, productive, ethical, and lawful manner.

This policy applies to work performed on a device on the Organization's behalf during working and nonworking hours, on and off of premises.

No Expectation of Privacy

All material, data, communications, and information, including but not limited to email (both outgoing and incoming), telephone conversations and voicemail, instant messages, and internet and social media postings and activities created on, received or transmitted by, printed from, or stored or recorded on the device for the Organization or on behalf of the Organization is the property of the Organization, regardless of who owns the device(s) used.

You are expressly advised that in order to prevent misuse, **the Organization reserves the right to monitor, intercept, review, and remotely wipe, without further notice, the entire contents of the device, including your personal content, in the Organization's sole discretion.** This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings, and other uses of the device, whether the device is in your possession or the Organization's possession. Therefore, you should have **no expectation of privacy whatsoever** in any of the Organization content.

Security Requirements – General

All devices used for the Organization's business or on behalf of the Organization must be registered with and authorized by [PERSON/POSITION] in the [DEPARTMENT NAME] Department.

To protect the Organization's confidential information from being lost or becoming public, you must immediately report any device used for the Organization's business or on behalf of the Organization that is lost, stolen, accessed by unauthorized persons, or otherwise compromised so the Organization can assess the risk and, if necessary, remotely wipe the entire contents of the device, including your personal content, in the Organization's sole discretion. You must also promptly provide the Organization with access to the device when requested or required for the Organization's legitimate business purposes, including in the event of any security incident or investigation.

The Organization's [INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS POLICY] applies to all uses of your device for the Organization's business or on behalf of the Organization. [In addition/To the extent the Organization's [INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS POLICY] does not address the issues below], you must:

- [Install [NAME OF SECURITY SOFTWARE] on the Organization's request and consent to the Organization's efforts to manage the device and secure its data, including providing the Organization with any necessary passwords or other means of accessing the device.]
- Comply with the Organization's device configuration requirements.
- Password protect the device through the use of strong passwords consistent with the Organization's current password policies and procedures.
- Maintain the device's settings such that the device locks itself and requires a password if it is idle for five minutes and use of the device is suspended after three failed login attempts.
- Maintain the device's original operating system and keep it current with security patches and updates.
- Not download or install software, including [SPECIFIED APPLICATIONS],] unless explicitly authorized by the Organization.
- Not alter the security settings of the device without the Organization's consent.
- Prohibit use of the device by anyone not authorized by the Organization, including your family, friends, and business associates.
- Not download or transfer work product or sensitive business content to your device, for example, via email attachments. You must erase any such information that is inadvertently downloaded to your device.
- Not back up or otherwise store the Organization content locally or to cloud-based storage or services without the Organization's consent. Any such backups or other stored copies of the Organization content inadvertently created must be deleted immediately. To the extent you create backups or otherwise store the Organization content with the Organization's consent, you must provide the Organization with access to your local or cloud-based storage to access and review any such backups or other stored copies of the Organization content when requested or required for the Organization's legitimate business purposes, including in the event of any security incident or investigation.
- Not use the device as a personal mobile hotspot without the Organization's consent.
- Not transmit any the Organization information over an unsecured Wi-Fi network.
- [ADDITIONAL PRECAUTIONS]

At all times, you must use your best efforts to physically secure the device against loss, theft, damage, or use by persons who have not been authorized to access the device by the Organization.

Appropriate Use

the Organization's policies prohibiting harassment, discrimination, and retaliation, namely apply to the use of all devices under this policy. You may not use any device in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs, or any other characteristic protected by applicable federal, state, or local law.

Nonexempt employees using their own devices under this policy must record all time spent working, including time spent using their own devices for work purposes during nonworking hours/are not permitted to use their devices for work purposes during nonworking hours [without prior written authorization from the Organization].

A new employee using their own device under this policy for the first time must erase all information related to any previous employment before using their device for the Organization's business or on behalf of the Organization.

Any employee who discontinues use of their device under this policy or leaves the Organization's employ must allow the Organization to remove the Organization content/the Organization's work product or sensitive business content from their device and to disable any software or services provided by the Organization on their device.

The Organization prohibits employees from talking, texting, emailing, or otherwise using a mobile or other electronic device, regardless of who owns the device, while operating the Organization vehicles, machinery, or equipment, or while operating personal vehicles, machinery, or equipment for the Organization's business or on behalf of the Organization. Employees must also comply with any applicable federal, state, or local law restricting the use of mobile or other electronic devices while operating vehicles, machinery, or equipment. For their own health and safety and the health and safety of others, employees should not use their devices while operating vehicles, machinery, or equipment of any kind.

Technological Support

The Organization does not provide technological support for employee devices. You acknowledge that you alone are responsible for any repairs, maintenance, or replacement costs and services.

Costs and Reimbursements

The Organization will reimburse employees a fixed amount for costs associated with their device usage for business purposes[, including a flat rate for any necessary repairs or replacement costs. Eligible employees will receive a reimbursement as follows:

- Voice services only: $[NUMBER] per month.
- Data services only: $[NUMBER] per month.
- Voice and data services: $[NUMBER] per month.
- [Repair and/or replacement costs: $[NUMBER] per [month/year/[TIME PERIOD]].]

To be eligible for reimbursement, you must send a copy of your monthly statement or bill substantiating your usage of the device for business purposes [and/or a copy of the bill or receipt substantiating any necessary repairs or replacement costs] to [PERSON/POSITION] within 30 days of your receipt of the invoice. If you are unable to obtain the invoice during a particular month, the employee may submit a signed written statement. Expenses beyond those listed above will not be reimbursed. For more information on device reimbursement procedures, please contact [PERSON/POSITION].

OR

The Organization will [reimburse employees for/provide employees with a stipend to cover] the total cost of their devices/partial cost of their devices [including any necessary repairs or replacement costs]. Additional costs beyond the stipend will not be reimbursed. For more information on [device reimbursement/stipend] procedures, please contact [PERSON/POSITION].]

Consequences for Failure to Comply

Employees who violate any provision of this policy are subject to discipline, up to and including termination of employment.

_____

Signature

_____

Printed Name

_____

Date]