**COMPANY: BYOD POLICY**

Employees at COMPANY are allowed to buy and use any smartphones or tablets they want for work-related purposes. If users don't follow the rules and guidelines listed below, COMPANY reserves the right to remove this privilege. The purpose of this policy is to safeguard the data security and technical infrastructure of Company. Due to differences in platforms and devices, a small number of exceptions to the rules may happen. To connect their devices to the corporate network, COMPANY workers must accept the terms and conditions outlined in this policy.

Acceptable Use

* Activities that directly or indirectly support corporation COMPANY’s operations are considered to be legitimate business use, according to the corporation.
* At the company's discretion, employees may not access specific websites during working hours or while connected to the corporate network.
* The company defines acceptable personal use on company time as reasonable and constrained personal communication or recreation, such as reading or gaming.
* While on-site, devices' cameras and/or video capabilities are/are not disabled.
* Devices may not be used at any time to transmit or store illegal materials, confidential information belonging to another firm, harass others, conduct unrelated business, etc.
* These applications are permitted: (Include a thorough list of the apps that are allowed, such as Facebook, Facebook Messenger, and productivity apps)
* Employees have access to the following company-owned resources via their mobile device: email, calendars, contacts, documents, etc.

Device and Support

* Smartphones are permitted, and this includes iPhones, Androids, Blackberries, and Windows phones (the list should be as specific as necessary, including models, operating systems, versions, etc.).
* Tablets, such as the iPad and Android tablets, are permitted (the list should be as comprehensive as possible, including models, operating systems, versions, etc.).
* IT supports connectivity issues; employees should/should not contact the device's maker or their carrier for problems with the operating system or hardware.
* Before accessing the network, devices must be handed to IT for correct job provisioning and configuration of common apps, such as browsers, office productivity software, and security tools.

Security

* Devices must be password protected utilizing the device's features to prevent unauthorized access, and a strong password is necessary to access the workplace network.
* If left idle for five minutes, the device locks itself using a password or PIN.
* The device will lock itself after five unsuccessful login attempts. IT must be contacted by staff members to reclaim access.
* It is highly forbidden for jailbroken or rooted (Android) devices to connect to the network.
* The company's list of supported devices for smartphones and tablets is/is not a list of devices that are permitted to connect to the network.
* Employees' personal use-only smartphones and tablets are/are not permitted to connect to the network.
* Access to company data is restricted for employees based on user profiles set by IT and automatically enforced.
* If the employee leaves the firm, the device is lost, a policy breach, a virus, or some similar threat to the safety of the company's data and technological infrastructure is discovered by IT, the device may be remotely erased.

Disclaimers

* It is the employee's obligation to take extra precautions, such as backing up email, contacts, and other personal data, even if IT will take all reasonable measures to avoid the employee's personal data from being lost in the event it must remotely wipe a device.
* The business retains the right to turn off services or disconnect equipment without warning.
* Device theft or loss must be notified to the business within 24 hours. It is the responsibility of the employee to contact the cell carrier right away if a device is lost.
* The employee is personally responsible for all expenses related to his or her equipment.
* The risk of losing company and personal data entirely or partially is fully assumed by the employee.
* For violations of this policy, Company ABC maintains the right to take necessary disciplinary action, up to and including termination.