Bring Your Own Device Policy

ABC COMPANY

BRING YOUR OWN DEVICE POLICY

1. **PURPOSE**

ABC Company follows a Bring Your Own Device ("BYOD") policy that allows employees to use their own personal smartphones and tablets to perform work duties. This BYOD Policy is intended to establish rules for employee behavior necessary to protect the privacy, security and integrity of ABC Company's data and technology infrastructure against the risks that can arise when employees use their personally owned devices for business purposes. ABC Company reserves the right to disconnect devices, disable services or otherwise revoke employees' BYOD privileges at any time and without notification if users fail to comply with the requirements and procedures set out in this Policy.

1. **BYOD DEVICES**

- The following devices and only the following devices are approved for employee BYOD use and connecting to the ABC Company network:
    - Android Smart Phones and Tablets
    - Blackberry Smart Phones and Playbook
    - iOS iPhones & iPads
    - [*List* others]
- Connectivity issues are supported by the ABC Company IT department. Employees [*must/may not*] contact their BYOD device manufacturer or carrier for operating system or hardware-related issues.
- Prior to accessing the ABC Company network, employees must present their BYOD devices to the IT department for job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

1. **NO EMPLOYEE EXPECTATION OF PRIVACY**

ABC Company will respect the privacy of your personal devices and take all reasonable precautions to keep it private and secure, ABC Company reserves the right to track and request access to the device to perform technical functions and implement security controls as outlined in this Policy. **Employees do not have the right and should not have the expectation of privacy while using BYOD equipment subject to this Policy.**

1. **ACCEPTABLE USES**

- Employees may use their BYOD devices for the acceptable business uses of ABC Company computers as set out in the ABC Company Computer Use Policy.
- Employees may not use their BYOD devices during work hours for personal purposes that are not permitted for use of ABC Company computers as set out in the ABC Company Computer Use Policy, e.g., BYOD devices may not be used for accessing pornographic or offensive materials, storing or transmitting ABC Company proprietary information, committing harassment, engaging in business activities that are in conflict of interest with their duties to ABC Company, etc.
- The following apps are permitted for downloading, installation and use on BYOD devices [*list*].
- The following apps are not permitted for downloading, installation and use on BYOD devices [*list*].
- While the IT department will take reasonable precautions to prevent the employee's personal data from being lost in the event it must remote wipe a BYOD device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

1. **EMPLOYEE OBLIGATIONS**

All employees participating in the BYOD program must take appropriate secure measures required for company devices under the ABC Computer Use Policy including but not limited to:

- Ensuring that their BYOD device is password protected using the features of the device and that a "strong password," as that term is defined in the ABC Company Computer Use Policy, is required to access the ABC Company network [*option: specifically list strong password requirements*];
- Ensuring that their BYOD device locks itself with a password or PIN if the device is idle for five minutes;
- Ensuring that their BYOD device locks itself and must be re-opened by the IT department after five failed login attempts;
- Not using rooted (Android) or jailbroken (iOS) devices to access the network;
- Not sharing their BYOD devices with friends, relatives or anybody other than a properly authorized user of the device under this BYOD Policy;
- Using their BYOD devices to access only the information authorized for that employee to access under the ABC Company authentication and authorization procedures;
- Reporting lost, misplaced or stolen BYOD devices to the IT department (and mobile carrier) within 24 hours;
- Paying all costs associated with purchasing and their BYOD device.

1. **REMOTE WIPING OF BYOD DEVICE**

The ABC Company IT department may remotely wipe an employee’s BYOD device may be remotely wiped if:

- The device is lost or stolen;
- The IT department detects a data or policy breach, virus or other threat to the security of ABC Company’s data and technology infrastructure; and/or

The employee’s employment is terminated.