Sample Bring Your Own Device (BYOD) Policy

The Organization grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. The Organization reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the Organization's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Organization employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the Organization network.

Acceptable Use

- The Organization defines acceptable business use as activities that directly or indirectly support the business of the Organization.
- The Organization defines acceptable personal use on working time as reasonable and limited personal communication or recreation, such as reading or game playing.
- The Organization does not define acceptable personal use on non-working time, such as break time, lunch time, and off-the-clock time because that is your personal time. Though, to the extent you are accessing social media sites, you are required to follow the Organization's Social Media Policy.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the Organization. Such websites include, but are not limited to the following non-exclusive list of websites:
    - Pornographic websites or other similar websites that contain illicit materials or materials of a sexual nature;
    - Online gaming websites;
    - Sites typically known to contain malware links;
    - Certain social media networking sites;
    - Others.
- Devices' camera and/or video capabilities [are/are] not disabled while on-site.
- Devices may not be used at any time to:
    - Store or transmit illicit materials;
    - Store or transmit proprietary information belonging to another Organization;
    - Harass others;
    - Engage in outside business activities;
    - Engage in any activity that would violate the Organization's policies;
    - Others.
- The following non-exclusive list of apps are allowed: *(include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)*
    - Weather apps;
    - Productivity apps;
    - Facebook,
- The following apps are not allowed:
    - Any app not downloaded through iTunes,
    - Gaming apps, including Candy Crush, Farmville, Angry Birds, and similar apps.
- Employees may use their mobile device to access the following Organization-owned resources: email, calendars, contacts, documents, etc.

- The Organization has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed *(the list should be as detailed as necessary including models, operating systems, versions, etc.).*
- Tablets including iPad and Android are allowed *(the list should be as detailed as necessary including models, operating systems, versions, etc.).*
- Connectivity issues are supported by IT; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

Reimbursement

- The Organization [will/will not] reimburse the employee for a percentage of the cost of the device (include the amount of the Organization's contribution), or the Organization will contribute X amount of money toward the cost of the device.
- The Organization will [pay the employee an allowance, cover the cost of the entire phone/data plan, pay half of the phone/data plan].
- The Organization will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

Security

- All devices used for the Organization's business or on behalf of Organization must be registered with and authorized by [PERSON/POSITION] in the [DEPARTMENT NAME] Department, inclusive of owner information and IP address(es).
- The employee must install applicable security software upon Organization's request and consent to Organization's efforts to manage the device and secure its data.
- The device must comply with Organization's device configuration requirements.
- Password protect the device through the use of strong passwords consistent with Organization's current password policies and procedures.
- The device must lock itself with a password or PIN if it is idle for five minutes.
- After five failed login attempts, the device will lock. Contact IT to regain access.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Employees are automatically prevented from downloading, installing and using any app that does not appear on the Organization's list of approved apps.
- Smartphones and tablets that are not on the Organization's list of supported devices [are/are not] allowed to connect to the network.
- Smartphones and tablets belonging to employees that are for personal use only [are/are] not allowed to connect to the network.
- Employees' access to Organization data is limited based on user profiles defined by IT and automatically enforced.
- Employee shall not back up or otherwise store the Organization's content [locally or] to cloud-based storage or services without Organization's consent. Any such backups or other stored copies of Organization content inadvertently created must be deleted immediately. To the extent you create backups or otherwise store Organization

content with Organization's consent, you must provide Organization with access to your [local or] cloud-based storage to access and review any such backups or other stored copies of Organization content when requested or required for Organization's legitimate business purposes, including in the event of any security incident or investigation.
- The employee's device may be remotely wiped if: (1) the device is lost; (2) the employee terminates his or her employment; (3) IT detects a data or policy breach, a virus or similar threat to the security of the Organization's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- The Organization reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the Organization within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the Organization's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Organization and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- The Organization reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

BRING YOUR OWN DEVICE (BYOD) POLICY

ACKNOWLEDGMENT

Employee Name: _____

Employee Position: _____

Date of Receipt of Bring Your Own Device (BYOD) Policy:

I acknowledge and agree that:

(1) I have received a copy of the Organization Bring Your Own Device (BYOD) Policy;

(2) I have read the Bring Your Own Device (BYOD) Policy in its entirety and fully understand the provisions contained therein; and

(3) I agree to abide by the provisions contained in the Bring Your Own Device (BYOD) Policy.

_____
Employee's Signature

_____
Employee's Name (Printed)

_____
Date