Date: 03/28/19

Version 1.0

BYOD Policy Template

# 1. 0 Purpose

To describe the conditions under which our employees my use their own devices at work. This policy covers mobile phones, tablets and laptops.

# 2.0 Policy

A. This Bring Your Own Device (BYOD) policy template provides standards and rules of behavior for the use of personally-owned smart phones, tablets, and/or laptops by our company. This template provides the structure of a BYOD policy and the mechanisms required to implement one. It is intended to protect the security and integrity of the company’s data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

## 3.0 Expectation of Privacy

A. Our company will respect the privacy of your personal device and will only request access to the device to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from our corporate policy for company provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using company equipment and/or services.

The policy isn’t just about protecting corporate data - it includes a program to keep personal employee data away from others, including our IT team. Our MDM (Mobile Device Management) solution will be uploaded on your personal device in order to parse data and manage access to certain data and service, such as:

* Personal emails, contacts, and calendars
* Application data and text messages
* Call history and voicemails

## 4.0 Acceptable Use

A. Acceptable use defines standards, procedures, and restrictions for employees who are connecting a personally-owned device to our organization’s network for business purposes. BYOD acceptable use applies to any hardware and related software that is not organizationally owned or supplied, but could be used to access organizational resources. That is, devices that employees have acquired for personal use but also wish to use in our business environment.

Date: 03/28/19

Version 1.0

BYOD Policy Template

The overriding goal of this policy is to protect the integrity of employee data and business data that resides within our company’s technology infrastructure. This policy intends to prevent data from being deliberately or inadvertently stored insecurely on a device or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to our company’s public image. Therefore, all employees using a personally-owned device connected to our organizational network, and/or capable of backing up, storing, or otherwise accessing organizational data of any type, must adhere to our company-defined processes for doing so.

It is acceptable to use company or personal devices to access the Internet during company time for a reasonable amount of time - less than 15 minutes. It is acceptable to use the device for limited personal communication or recreation such as reading, texting or playing games. Devices may not be used at any time to:

* + Store or transmit illicit materials
  + Store or transmit proprietary information
  + Harass others
  + Engage in outside business activities.

Employees may use their mobile device to access the following company-owned resources:

* + Email
  + Calendars
  + Contacts
  + Documents

## 5.0 Devices and Support

A. This section defines the devices and applications covered by our BYOD policy. Our company will load the MDM software on your device and provide support services.. This includes any smart mobile devices and tablets that are owned by the employee and used for business purposes. We expect you to use company laptops and PCs to perform all work-related activities rather than your personal laptop.

The following classifications of media are ones that can be considered:

* Smartphones
* Other mobile/cellular phones
* Tablets
* Portable media devices
* PDAs

## 6.0 Monitoring Standard

A. Wireless networks shall be monitored to detect intrusions by unauthorized wireless devices. This shall be accomplished either through a wireless control system that identifies unauthorized devices in real-time, or via periodic scans for rogue WAPs. These scans shall be documented to provide evidence of the date of the scan, results of the scan, and any actions that were taken as a result of the scan.

# 7.0 Applicability

A. This policy is applicable to all users - employees, customers and affiliates who are on site.

# 8.0 Other Applicable Policies

A. None

Date: 03/28/19

Version 1.0

BYOD Policy Template

B. Provisioning Your Device for Company Use. Contact our IT team or team leader who will provision your device. Our IT team will download the MDM application to your device and provide you instructions on login and password setup. Once configured, you should be able to perform your daily work activities and have our security team monitor the device use. Should any technical issues arise, you should contact <insert responsible party>. For network issues and issues with our proprietary software (if you have one), our company will be responsible for correcting, however, you are responsible for any hardware or software issues of your device. The following devices are supported:

iPhone (3GS, 4, 4S, 5, etc.…)

iPad (<list acceptable operating systems>)

Android (Samsung Galaxy S6, S7, etc...)

<Describe the devices supported>

For connectivity issues - contact our IT team. For device related issues contact your device manufacturer or your carrier for operating system or hardware issues. Employee devices to be used under our BYOD policy must be provided to IT for proper provisioning and configuration of our apps, browsers, office productivity software and security tools, before you can access the network.

## 6.0 Security

This section describes the security for our BYOD policy. This policy defines which applications and resources employees can access via their mobile devices.

(NOTE: The security team can develop system threat models for mobile devices and the resources that are accessed through the devices. The guidelines should be derived from those policies.)

The following describes our mobile device security guidelines:

* In order to prevent unauthorized access, devices must be password protected using the features of the device in order to access the company network.
* The company’s strong password policy is: Passwords must be at least eight characters and a combination of upper and lower case letters, numbers and symbols. Passwords will be rotated every 90 days and the new password can’t be one of 15 previous passwords.
* The device must lock itself with a password or PIN if it’s idle for five minutes.
* Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
* Smartphones and tablets that are not on the company’s list of supported devices are not allowed to connect to the network.
* Smartphones and tablets belonging to employees that are for personal use only (without MDM installed) are not allowed to connect to the network.

Date: 03/28/19

Version 1.0

BYOD Policy Template

Employees’ access to company data is limited based on their user profile, defined by their supervisor and implemented by IT. The employee’s device may be remotely wiped if:

* The device is lost or stolen.
* The employee terminates his or her employment.
* IT detects a data or policy breach, a virus or similar threat to the security of the company’s data and technology infrastructure.

**7.0 Reimbursements**

Reimbursements may be considered as appropriate for device or data usage, and should be discussed with your supervisor. If you are approved for a reimbursement, the following applies:

* The company will/will not reimburse the employee for a percentage of the cost of the device (include the amount of the company’s contribution), or, the company will contribute X amount of money toward the cost of the device. (Decide which statement applies.)
* The company will a) pay the employee an allowance, b) cover the cost of the entire phone/data plan, c) pay half of the phone/data plan. (Decide which condition applies.)
* The company will/will not reimburse the employee for the following charges: roaming, plan overages, etc. (Decide which condition applies.)

**8.0 Disclaimer**

This section is a disclaimer for any risks that may exist with this BYOD policy. In general, the company is not responsible for misuse of a device or damages to a device that occur during normal operation.

* While IT will take every precaution to prevent the employee’s personal data from being lost, in the event it must remotely wipe a device, it is the employee’s responsibility to take additional precautions, such as backing up email, contacts, etc.
* The company reserves the right to disconnect devices or disable services without notification.
* Lost or stolen devices must be reported to the company 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 company’s acceptable use policy and other applicable policies.

# 7.0

,

BYOD Policy Template

Date: 03/28/19

Version 1.0

* 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 company 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.
* <Company Name> reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy

# 9.0 Applicability

A. This policy is applicable to all employees.

# 10.0 Other Applicable Policies

A. See our Privacy and Cybersecurity Policies

# User Acknowledgment and Agreement

By signing below, you agree to comply with this BYOD policy.

*I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of <Company Name> services. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business related data/voice plan usage of my personal device is not provided. (Assuming the company opts not to reimburse employee for usage for business purposes)*

Employee Name:

BYOD Device(s):

Employee Signature: Date: