BYOD Policy & Agreement

Definitions

Bring Your Own Device (BYOD): Privately owned wireless and/or portable electronic handheld equipment.

Overview

This policy establishes [Company Name] guidelines for employee use of personally owned electronic devices for work-related purposes.

Acceptable use of BYOD at [Company Name] must be managed to ensure that access to [Company Name]'s resources for business are performed in a safe and secure manner for participants of the [Company Name] BYOD program. A participant of the BYOD program includes, but is not limited to:

- Employees
- Contractors
- Board of Directors
- Volunteers
- Related constituents who participate in the BYOD program

Scope

Employees of [Company Name] may have the opportunity to use their personal electronic devices for work purposes when authorized in writing, in advance, by the employee and management. Personal electronic devices include personally owned cell phones, smartphones, tablets, laptops and computers.

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data using their personal device. This policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the [Company Name] BYOD program which contains stored data owned by [Company Name], and all devices and accompanying media that fit the following device classifications:

- Laptops
- Tablets
- Mobile/cellular phones, including smartphones
- Any non-[Company Name] owned mobile device capable of storing corporate data and connecting to an unmanaged network

The use of personal devices is limited to certain employees and may be limited based on compatibility of technology. Contact the human resource (HR) department for more details.

Audience

This policy applies to all [Company Name] employees, including full and part-time staff, Board of Directors, volunteers, contractors, freelancers, and other agents who utilize personally-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data.

Such access to this confidential data is a privilege, not a right, and forms the basis of the trust [Company Name] has built with its members, suppliers, and other constituents.

Consequently, employment at [Company Name] does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Protocols

To ensure the security of [Company Name] information, authorized employees are required to have antivirus and mobile device management (MDM) software installed on their personal mobile devices. This MDM software will store all company-related information, including calendars, e-mails and other applications in one area that is password-protected and secure. [Company Name]'s IT department must install this software prior to using the personal device for work purposes.

Employees may store company-related information only in this area. Employees may not use cloud-based apps or backup that allows company-related data to be transferred to unsecure parties. Due to security issues, personal devices may not be synchronized with other devices in employees' homes. Making any modifications to the device hardware or software beyond authorized and routine installation updates is prohibited unless approved by IT. Employees may not use unsecure Internet sites.

All employees must use a preset ringtone and alert for company-related messages and calls. Personal devices should be turned off or set to silent or vibrate mode during meetings and conferences and in other locations where incoming calls may disrupt normal workflow.

We also require all employees to adhere to the following security protocols:

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network.

- The company's strong password policy is: Passwords must be at least six 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.
- 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 company's list of approved apps.
- Smartphones and tablets that are not on the company'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 company data is limited based on user profiles defined by IT and automatically enforced.
- 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 company's data and technology infrastructure.

Policy Detail

This policy applies to:

- Any privately owned wireless and/or portable electronic handheld equipment, hereby referred to as BYOD. [Company Name] grants potential participants of the BYOD program the privilege of purchasing and using a device of their choosing at work for their convenience.
- Related software that could be used to access corporate resources.

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

The Audience, as defined above, must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network. If users do not abide by this policy, [Company Name] reserves the right to revoke this privilege.

Eligibility

The following criteria will be considered initially, and on a continuing basis, to determine if the Audience is eligible to connect a personal smart device to the [Company Name] network.

- Management's written permission and certification of the need and efficacy of BYOD for that Employee
- Sensitivity of data the Audience can access
- Legislation or regulations prohibiting or limiting the use of a personal smart device for [Company Name] business
- Must be listed on the Information Technology Department's list of approved
- mobile devices
- Audience's adherence to the terms of the Bring Your Own Device Agreement and this policy and other applicable policies
- Technical limitations
- Other eligibility criteria deemed relevant by [Company Name] or IT

Roles and responsibilities

Responsibilities of [Company Name]

- IT will centrally manage the BYOD program and devices including, but not limited to, onboarding approved users, monitoring BYOD connections, and terminating BYOD connections to company resources upon the users leave of employment or service to [Company Name].
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable.
- IT reserves the right to refuse, by non-physical means, the ability to connect mobile devices to [Company Name] and [Company Name]-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts [Company Name]'s systems, data, users, and members at risk.
- IT will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to the [Company Name] infrastructure. To find out if a preferred device is on this list, an individual should contact the [Company Name] IT department Service Desk. Although IT currently allows only listed devices to be connected to the [Company Name] infrastructure, IT reserves the right to update this list in the future.
- IT will maintain enterprise IT security standards.
- IT will inspect all mobile devices attempting to connect to the [Company Name] network through an unmanaged network (i.e. the Internet) using technology centrally managed by the IT Department.
- IT will install the Mobile VPN software required on Smart mobile devices, such as Smartphones, to access the [Company Name] network and data.

[Company Name]'s IT Department reserves the right to:

- Install anti-virus software on any BYOD participating device
- Restrict applications
- Limit use of network resources
- Wipe data on lost/damaged devices or upon termination from the BYOD program or [Company Name] employment
- Properly perform job provisioning and configuration of BYOD participating equipment before connecting to the network
- Through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the [Company Name] network

Third party vendors
Third party vendors are expected to secure all devices with up-to-date anti-virus signature files and anti-malware software relevant or applicable to a device or platform. All new connection requests between third parties and [Company Name] require that the third party and [Company Name] representatives agree to and sign the Third Party Agreement. This agreement must be signed by the Vice President of the sponsoring department, as well as a representative from the third party who is legally empowered to sign on behalf of the third party. By signing this agreement, the third party agrees to abide by all referenced policies. The document is to be kept on file. All non-publicly accessible information is the sole property of [Company Name].

Safety
This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

This policy addresses a range of threats to, or related to, the use of [Company Name] data:

Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware and other threats could be introduced via a mobile device
Compliance	Loss or theft of financial and/or personal and confidential data could expose [Company Name] to the risk of non-compliance with various identity theft and privacy laws

Employees are expected to follow applicable local, state and federal laws and regulations regarding the use of electronic devices at all times.

Employees whose job responsibilities include regular or occasional driving are expected to refrain from using their personal devices while driving. Regardless of the circumstances, including slow or

stopped traffic, employees are required to pull off to the side of the road and safely stop the vehicle before placing or accepting a call or texting. Special care should be taken in situations involving traffic, inclement weather or unfamiliar areas.

Employees who are charged with traffic violations resulting from the use of their personal devices while driving will be solely responsible for all liabilities that result from such actions.

Employees who work in hazardous areas must refrain from using personal devices while at work in those areas, as such use can potentially be a major safety hazard.

Lost, stolen, hacked or damaged equipment
Employees are expected to protect personal devices used for work-related purposes from loss, damage or theft.

In an effort to secure sensitive company data, employees are required to have "remote-wipe" software installed on their personal devices by the IT department prior to using the devices for work purposes. This software allows the company-related data to be erased remotely in the event the device is lost or stolen. Wiping company data may affect other applications and data.

[Company Name] will not be responsible for loss or damage of personal applications or data resulting from the use of company applications or the wiping of company information. Employees must immediately notify management in the event their personal device is lost, stolen or damaged. If IT is unable to repair the device, the employee will be responsible for the cost of replacement.

Employees may receive disciplinary action up to and including termination of employment for damage to personal devices caused willfully by the employee.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the [Company Name] network.

Termination of employment
Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection. All company data on personal devices will be removed by IT upon termination of employment.

Violations of policy

Employees who have not received authorization in writing from [Company Name] management and who have not provided written consent will not be permitted to use personal devices for work purposes. Failure to follow [Company Name] policies and procedures may result in disciplinary action, up to and including termination of employment.

Restrictions on authorized use

Employees whose personal devices have camera, video, or recording capability are restricted from using those functions anywhere in the building or on company property at any time unless authorized in advance by management.

While at work, employees are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices. [Company Name] policies pertaining to harassment, discrimination, retaliation, trade secrets, confidential information and ethics apply to employee use of personal devices for work-related activities.

Family and friends should not use personal devices that are used for company purposes.

Privacy & company access

No employee using his or her personal device should expect any privacy except that which is governed by law. [Company Name] has the right, at any time, to monitor and preserve any communications that use the [Company Name]'s networks in any way, including data, voice mail, telephone logs, Internet use and network traffic, to determine proper use.

Management reserves the right to review or retain personal and company-related data on personal devices or to release the data to government agencies or third parties during an investigation or litigation. Management may review the activity and analyze use patterns and may choose to publicize these data to ensure that [Company Name]'s resources in these areas are being used according to this policy. Furthermore, no employee may knowingly disable any network software or system identified as a monitoring tool.

Help & support

[Company Name]'s IT department is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software.

(This applies even to devices already known to the IT department.)

Disclaimer

[Company Name] expressly disclaims, and the User releases [Company Name] from, all liability for any loss, cost, or expense of any nature whatsoever sustained by the User in connection with the privilege afforded the User under the terms of the Agreement.

Please sign and return the attached BYOD agreement.

Bring Your Own Device (BYOD) Agreement

I have read and understand [Company Name]'s BYOD Policy, and I understand the requirements and expectations of me as an employee.

Employee Signature:

_____

Date: _____