BYOD Policy Template

By Megan Berry

Bring your own device (BYOD) programs call for three critical components: a software application for managing the devices connecting to the network, a written policy outlining the responsibilities of both the employer and the users, and an agreement users must sign, acknowledging that they have read and understand the policy.

Writing a BYOD policy forces companies to think things through before they turn their employees loose with their own smartphones and tablets on the organization's network. Questions that must be settled by the organization's leadership during the planning stage include: Which web browsers should employees use? Which security tools offer the best protection for the range of devices that will be allowed to connect to the network? What level of support is IT expected to provide? To make sure nothing is overlooked, get input from people across the company: HR, IT, accounting, legal – workers and executives alike.

Below is a sample BYOD policy template that organizations can adapt to suit their needs (include additional details where it makes sense). Some companies may need to add sections that apply to different user groups with varying job requirements. Finally, be sure to have legal counsel review it.

Company XYZ: BYOD Policy

Company XYZ grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience. Company XYZ 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 Company XYZ's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

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

Acceptable Use

- The company defines acceptable business use as activities that directly or indirectly support the business of Company XYZ.
- The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.
- Employees are blocked from accessing certain websites during work hours/while connected to the corporate network at the discretion of the company. Such websites

include, but are not limited to…

- 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 company
  - Harass others
  - Engage in outside business activities
  - Etc.
- The following apps are allowed: (include a detailed list of apps, such as weather, productivity apps, Facebook, etc., which will be permitted)
- The following apps are not allowed: (apps not downloaded through iTunes or Google Play, etc.)
- Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
- Company XYZ 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 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.
- 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, etc.
- The company will/will not reimburse the employee for the following charges: roaming, plan overages, etc.

Security

- 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.

The Data Center Build-or-Buy Decision: 6 Key Factors You Should Consider

Video Conferencing: In the Cloud, Or On Your Premises?

TOP TRENDING RESOURCES

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 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 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 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 XYZ reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

For help with other IT policies, be sure to read our:

- Password policy template
- Cloud computing policy template, and
- Social networking policy template.