Bloomberg BNA

Privacy and Security Law Report®

BYOD Policies

As employees more and more use their personal devices for work purposes and corporate bring your own device policies touch on technologies associated with the devices, the policies should consider specific internal department stakeholders, including human resources, legal, information technology and facilities, the authors write.

Bring Your Own Device Policy Language and Considerations for HR, Legal, IT and Facilities Stakeholders



By Emily R. Fedeles, James A. Sherer and Judy Selby

Emily R. Fedeles serves as an associate at BakerHostetler in New York.

James A. Sherer serves as counsel at BakerHostetler in New York.

Judy Selby serves as partner at BakerHostetler in New York.

The views expressed herein are solely those of the authors; they should not be attributed to their places of employment, colleagues, or clients; and they do not constitute solicitation or the provision of legal advice.

Introduction

When an organization decides to implement a ''bring your own device'' (BYOD) program, or recognizes that current practices have evolved such that the organization is already effectively running this type of program and decides to formalize the process, we strongly advise the organization to draft and implement a policy to manage that activity. While a BYOD policy will certainly touch on technologies associated with the devices themselves, it should also consider a variety of specific internal stakeholders, which generally include at least (but certainly may not be limited to) the following departments: Human Resources, Legal, Information Technology (IT) and Facilities.

This article focuses on BYOD issues associated with these specific stakeholders and outlines some of their

 ISSN 1538-3423

relevant concerns with respect to a BYOD program. As a general principle, however, these groupings might apply to different and more specific organizational divisions, depending on the size and layout of the organization. Further, because a BYOD policy must be industry—and organization—specific, it is simply impossible to draft a one-size-fits-all policy that is generally applicable across the board. Instead, this article offers examples of form language that an organization may consider incorporating into various points within its BYOD policy.

Of course, because of the rate at which both technology and the legal landscape evolve, it is imperative that organizations regularly review and, when necessary, update their policies.

Specific Stakeholder Considerations

Human Resources Department

- Employee Handbook
  - o Which mobile devices will the organization support?
    - Do employees have an open-ended choice or will they be limited to choosing from a list provided by the organization? *[The following devices are approved for use: iPhone (list acceptable models), iPad (list acceptable models), BlackBerry (list acceptable models). . .]*
    - Are all versions, models and operating systems on those devices supported, or are only certain ones? *[The following operating systems are approved for use: iOS (list acceptable versions), Android (list acceptable versions). . .]*
  - o Who is eligible to participate?
    - Are all employees eligible to participate?
    - Are only employees with certain job functions eligible to participate? *[Employees with the following titles are eligible to participate in the BYOD program: (list acceptable titles). Other employees may be eligible to participate subject to approval by _____.]*
- Acceptable Use Policy
  - o To what extent, if any, will the organization attempt to restrict use of the BYOD device?
    - Will there be restrictions prohibiting the employee from using it for personal use? *[Employees should keep personal calls, e-mails, and other communications on BYOD devices during the workday to a minimum.]*
    - Will it restrict any user but the employee accessing it? *[Family and friends are not permitted to use BYOD devices for personal use. Any remote wiping procedures and related costs associated with these types of access are the employee's responsibility.]*
  - o Will the organization allow the device to be synchronized with other devices, e.g., a personal tablet at an employee's home? *[An employee is prohibited from synchronizing a BYOD device with other personal devices not utilized in a BYOD capacity.]*
    - What about backup methods? *[An employee is prohibited from using backup methods that allow company-related data to be transferred to unsecure parties.]*
  - o What behavior is strictly prohibited in conjunction with other organizational policies, e.g., harassment? Texting and driving? Talking and driving? Storing and transmitting illicit materials? *[Employees are strictly prohibited from using BYOD devices in the following manner at any time: harassing others, storing and transmitting illicit materials; texting and driving; talking while driving unless using a hands-free device. . .][Organizational policies pertaining to (list policies, e.g., harassment, discrimination, retaliation, ethics. . .) apply to BYOD devices for work-related activities at all times.]*
  - o Which applications are required on the BYOD device? *[Employees utilizing the BYOD program are required to install the following applications: (list required applications: security ''remote wipe'' program, VPN instance, etc.).]*
  - o Which applications are permitted on the BYOD device? Which ones are banned? *[Employees are permitted to access the following company-owned resources: (list acceptable resources: email, calendars, contacts, etc.). They are prohibited from visiting the following applications: (list banned areas, e.g., social media sites, etc.).]*
  - o Will the organization prevent the employee from using the BYOD device to access certain websites during work time/while connected to the corporate network? *[Employees are prohibited from accessing the following websites on their BYOD devices during work time/while connected to the corporate network: (list forbidden websites).]*
  - o How should the organization inform employees of applicable policies and verify acknowledgement and understanding of such policies? *[All employees are required to read and sign the BYOD policies prior to being allowed to participate in the program. Employees will be required to acknowledge the policy each time it is updated as well review it every ____ months.]*
  - o How will the organization handle policy violations? *[Employees who have not received authorization in writing from the organization's management and who have not provided written consent/acknowledgment of the policy will not be permitted to use BYOD devices for work purposes. Failure to follow the applicable policies may result in disciplinary action, up to and including termination of employment.]*
- Compensation
  - o Will the organization reimburse the employee for the cost of purchasing the device or related accessories? *[The organization will/will not reimburse the employee for the cost of purchasing*

  PVLR ISSN 1538-3423

the device and/or related accessories, such as cases, replacement batteries, etc.]

- o Will the organization reimburse the employee for the cost of purchasing software or software licenses for the device, including those programs the employee already uses at work? *[The organization will/will not reimburse the employee for the cost of purchasing additional software licenses for the device; such software is limited to the following (list types and versions).]*
- o Will the organization pay for data plan charges? *[The organization will reimburse/provide a stipend for all/a set portion of the data charges based on the employee's seniority. The stipend/reimbursement will be provided monthly/bi-monthly, etc.]*
  - ■ If so, will they do so via reimbursement or a set stipend?
  - ■ Will they reimburse a portion or the entire amount?
  - ■ Will the organization offer a choice between services that distinguish data usage on a per-app or utilization basis (e.g., Exchange ActiveSync, Good for Enterprise)?
- o Will standard charges be treated differently from overages, roaming charges, international charges or other such expenses?
- o Does applicable law require consideration of overtime and other wage-and-hour restrictions with respect to BYOD use outside of normal working hours?

Legal Department

- ■ If the organization needs to collect information from the device—either for business purposes, or to comply with law or legal process—what additional considerations arise?
  - o Is the organization required to segregate certain information prior to, or following, collection?
  - o How will the organization respect employee's privacy rights during collections? *[If the organization needs to collect information from the device, it will make attempts to segregate work-related information during/after collection, but the employee acknowledges that this may not always be possible.]*
- ■ Does the organization have the right to audit employee use of BYOD devices or access certain functions of the devices?
  - o Does the organization have the right to examine now-standard GPS data, health and welfare data (such as recent iPhone functionality for step and stair counts) that the employee would be required to opt-out of if even aware? *[The organization retains the right to examine employee BYOD devices under the following circumstances (list)]*
  - o Does the organization have the right to examine data collected or processed by employee-added applications whether or not such applications are prohibited by policy? *[The organization retains the right to examine employee BYOD devices in order to support proper employee BYOD device usage, data collection, processing, storage, and data use.]*
  - o Does the organization have the right to examine employee devices in order to assist employees in understanding how certain applications collect, process, store and use data in ways the employee may not be aware of? *[The organization retains the right to examine employee BYOD devices in order to support proper employee BYOD device usage, data collection, processing, storage and data use.]*
- ■ When does the organization have the right to monitor and preserve communications on BYOD devices?
  - o At all times? Or only as a consequence of a legal hold, an investigation, or the like?
  - o What is subject to monitoring and preserving, e.g., data, voicemail, etc? *[The organization will only monitor and preserve work-related communications as a consequence of a legal hold, (list other applicable situations). The type of communications monitored may include the following: (list all applicable communications). The employee may not always be notified of the organization's monitoring/preserving efforts.]*
- ■ Will the organization need to restrict the use of BYOD devices for certain types of *work* activity, for example, when legal holds create preservation and collection burdens? *[During certain situations, such as (list applicable situations, e.g., legal hold), the organization may instruct an employee not to use his/her BYOD device for work-related purposes.]*
- ■ How will the organization address border crossing security issues with respect to BYOD devices? *[Every employee must notify the organization prior to using its BYOD device in another country. The organization reserves the right to prohibit the employee from taking the BYOD device across a border. If the trip is a work-related one, the organization may supply the employee with temporary means of accessing work-related materials.]*

IT Department

- ■ Which Mobile Device Management Solutions (MDMs) provide the most necessary and appropriate security for the organization? *[BYOD devices must have the following organization-approved MDM software suite installed.]*
  - o Who installs this software? *[The IT department is responsible for installing and configuring any required applications, software, and security tools. Installation must be completed prior to an employee signing onto the organization's network with his/her BYOD device. Making any modifications to this software beyond routine updates is prohibited unless approved by the IT department.]*

- If an organization pays for the device directly, which party will be considered the ''customer'' in the relationship with the service provider?
- How many devices are employees allowed to use under the policy?
- To what extent will the organization seek to segregate business data from personal data on the device—and what if such segregation is not technologically feasible?
- When will the organization utilize a remote wiping policy? *[The organization will remotely wipe a device in the follow situations:]*
  - o Employee separation and device decommissioning/disposal *[When employment is terminated.]*
    - What heightened security measures are needed if an employee is terminated or otherwise separates from the company on bad terms?
  - o Lost or stolen device *[When the BYOD device is lost or stolen.]*
    - What reporting time limits are in place? *[An employee is required to report a lost or stolen device within ____ hours/days.]*
  - o Data breach, virus or similar security threat *[When the IT department detects or is notified about a data or policy breach, a virus, a security threat. . . .]*
  - o What notification period, if any, will the organization give an employee before utilizing a remote wiping policy? *[The IT department is not required to give an employee notice prior to remote wiping the BYOD device/the IT department will provide an employee with ___ hours' notice prior to remote wiping the BYOD device.]*
  - o What precautions, if any, will the organization take to prevent an employee's personal data being lost during the remote wipe process? *[While the IT department 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 the devices in a secure manner.]*
- What measures are in place for recovery of company data if it is inadvertently or intentionally deleted from a BYOD device? *[In the instance of deletion of company data from a BYOD device, the IT department will _____. If the deletion is intentional, the employee will face disciplinary consequences according to the employee handbook.]*
- What protection will the organization require to prevent unauthorized access? *[To protect unauthorized access, the organization requires the following safeguards:]*
  - o Strength of password? *[A strong password, which is defined as a password at least ___ characters in length, a combination of upper- and lower-case letters,. . .]*
  - o Password rotated and ban on using prior passwords? *[A password that must be rotated every ___ days, with the new password prohibited from being one of the ___ previous passwords.]*
  - o Automatic locking after a certain period of idle time? *[The device must lock itself with this strong password if it is idle for ___ minutes.]*
  - o Automatic wiping after an incorrect passcode is entered too many times? *[The device will be wiped if an incorrect passcode is entered ___ times.]*
  - o Prohibiting jailbroken or rooted devices from accessing the network? *[Jailbroken (iOS) or rooted (Android) devices are forbidden from accessing the network.]*

Facilities Department

- Are there certain physical areas of the organization where BYOD devices may not be used? *[Employees are prohibited from using BYOD devices in the following areas at any time/at certain designated times: _____.]*
- Will the organization restrict or prohibit BYOD camera/video/recording capabilities anywhere in certain zones, buildings, or in certain areas of a given building? *[Employees whose BYOD devices have camera, video, or recording capability are restricted from using those functions in ____ areas at any time/at certain designated times unless authorized in advance by _____. Such devices may be confiscated prior to entry and returned to employees at a later time.]*

User Acknowledgement and Agreement

I, (Employee Name), acknowledge, understand, and will comply with the above referenced policy and rules of behavior, as applicable to my approved BYOD device usage.

Employee Name: _____
BYOD Device(s): _____
Employee Signature _____
Date: _____

  PVLR ISSN 1538-3423