DJC Oregon
Oregon's Building Connections

OP-ED: A checklist for an effective BYOD policy

By: Fallon Niedrist in Focus on Law | November 20, 2015 3:22 pm


Fallon Niedrist

"Bring Your Own Device" (BYOD) workplace policies can offer a lot of benefits to both employees and employers. Employees get the satisfaction of using their preferred device and not having to carry both a personal and work-issued device, and employers can enjoy the benefit of shifting costs to employees.

However, a recent survey shows that the BYOD trend has waned. Even compared to two years ago, more employers are providing employees with devices and banning the use of personal devices for work. This trend is likely the result of employers weighing the risks of employees using their own devices for work – including security breaches, electronic discovery problems, and even wage and hour liability – and coming down against BYOD.

However, with a strong policy in place, an employer can mitigate the associated risks while still maintaining the benefits of employees supplying their own devices. Here is a practical checklist of key issues to consider when implementing a BYOD policy.

Informed consent

Employees' informed consent before participating in BYOD is key to any effective policy. Employers should fully explain their practices and ensure that employees understand and consent, in writing, to those practices before allowing them to use their own devices for work.

Information privacy laws

Employers should consider whether they are subject to any data privacy and security laws. For example, health care companies may be subject to the HIPAA confidentiality requirements, and financial services companies may be subject to the privacy provisions of the Gramm-Leach-Bliley Act. These privacy requirements will need to be addressed in a BYOD policy.

Trade secrets and confidential information

Do employees have access to trade secrets or confidential information? If so, ensure they understand how their confidentiality restrictions intersect with their use of their personal devices.

Consideration of who can use devices

Think carefully before allowing employees who must be paid overtime (i.e., non-exempt ones) to use their own devices for work purposes. If employees use their devices to check email or work off the clock, an employer might be liable for any unpaid overtime worked by employees even if they were previously instructed not to do so.

Permitted and prohibited devices and software

Employers should state which device brands, models and software are allowed under the policy. Restricting types of devices can help ensure compatibility with company-issued devices, and restricting software can eliminate security risks.

Employers also can require employees to place information management software on their devices, so long as they inform the employees what information the software has access to and how the company uses the software. Further, employers should require employees to work with their IT department to enroll in the BYOD program, receive security updates, agree to remote access to the device, install specific software, and receive continuous support.

Employee responsibilities

An employer's policy should outline employees' obligations while using their own devices for work. For example, the policy should include instructions on reporting a lost or stolen device; how time worked remotely should be recorded; an express statement of who is responsible for costs, including the purchase of the device, replacement costs, repairs, service, etc.; and exit requirements when an employee leaves the company, including deleting data, revoking access to a network, deleting certain apps, or turning over the device to the employer to perform necessary tasks.

Employee consent to security practices

Employees must be informed about the employer's security practices and must consent to those practices. For example, the policy should include the company's remote data deletion policy, including the circumstances under which data may be deleted remotely and what kinds of information may be deleted – potentially including both company and personal data. The policy also should specify what level of access the employer has to personal data on a device, including whether it accesses personal content on employees' devices and employees' expectations of privacy.

Finally, the policy should make clear the employer's litigation hold practices, including employees' obligation to follow company data retention policies, and what an employee should do in the event a litigation hold is issued by the company.

These considerations can help identify key issues for both determining whether BYOD is right for a workplace and putting an effective policy in place.

Fallon Niedrist is an attorney in the Portland office of Fisher & Phillips LLP, which is dedicated to representing the interests of management. Contact her at fniedrist@laborlawyers.com or 503-205-8094.