PUBLICATION

BYOD Programs: Ensuring the Savings are Worth the Risks

Authors: Jennie Vee Silk
May 22, 2019

Many employers are moving towards a "Bring Your Own Device" (BYOD) program, in which employees are allowed to connect their own personal cell phones, iPads, and laptops to the employer's network and systems. A BYOD program differs from a program in which company-owned electronic devices are permitted to access the employer's network and data. While a company-owned device program allows an employer to maintain maximum security and control over its networks and systems, the cost of providing employees with company-owned electronic devices is exorbitantly high.

There is no question that a BYOD program can save an employer money; however, there are several security, legal, privacy, and administrative issues an employer must consider before implementing a BYOD program.

- Security. Data and network security is a primary concern for an employer implementing a BYOD program. The employer should implement an enterprise-wide written information security program to address issues such as unsecured Wi-Fi networks, password-protection, reporting loss or theft, update/patch requirements, remote wipe after a specified number of failed log-in attempts, and encryption requirements.

  Additionally, certain employers must implement a data breach response program under the Health Insurance Portability and Accountability Act (HIPAA), the Gramm–Leach–Bliley Act (GLBA), and certain states' data security requirements.

- Legal. There are several legal issues implicated by a BYOD program. BYOD and personal communication devices can further blur the lines between personal and work time, raising the issue of whether time is compensable under the Fair Labor Standards Act and state law. In addition to wage and hour concerns, the use of personal devices to conduct job-related tasks creates an opportunity for employees to store proprietary company information on their personal device. Additionally, if the employer is involved in litigation, the employee's device must be accessible in the course of discovery. Furthermore, workplace harassment, discrimination, and privacy risks are not avoided because suspect activities happen on an employee's device, rather than the company's device. Lastly, an employer considering a BYOD program for a group of employees represented by a bargaining group likely will need to bargain with the union on whether it can implement such a program.

- Privacy. Another issue employers must confront before implementing a BYOD program is the employee's expectations of privacy with their personal electronic device. The employer's BYOD policy should reserve the right to monitor all work-related communications and activity on the employee's electronic device. It should be clear, however, that participation in the BYOD program is voluntary, and the employer's BYOD policy should be posted and accessible to all employees.

- Administrative. The employer's BYOD policy should outline what devices are permitted and whether the employer's IT department will service/troubleshoot the employee's device. Additionally, the employer should use device-management software, such as MobileIron, that allows the employer to

maintain some control over the device. The policy should also address whether the employee is eligible for reimbursement for monthly cell phone charges. Finally, a sound BYOD policy should include an exit strategy for wiping company data from the device in the event of a separation from the employee.

While the risks and pitfalls of a BYOD program are significant, they can be largely mitigated or eliminated by the implementation of a strong BYOD policy that protects the employer's data, clearly outlines the terms for the employees, and addresses all potential legal issues.

For additional information about BYOD programs or for assistance implementing a BYOD policy for your employees, please contact Jennie Vee Silk, or any member of Baker Donelson's Labor & Employment Group.