BYOD in the workplace

Creating bring your own device policies to mitigate risks

CHRISTINA D. FRANGIOSA
Attorney
Semanoff Ormsby Greenberg & Torchia, LLC

cfrangiosa@sogtlaw.com
(267) 620-1902

Insights Legal Affairs is brought to you by **Semanoff Ormsby Greenberg & Torchia, LLC**

Many companies today allow employees to use their personal smartphones or mobile devices to perform company business and access company data. While allowing dual-use devices may result in lower costs to a company initially, failing to plan for potential risks can be very costly in the long term.

Before a company allows employee-owned devices to be used for work purposes, a bring your own device (BYOD) policy should be created that's specifically tailored to the company's business and explains its expectations and practices.

"Rules relating to security and privacy can help protect a company's confidential data, but rules addressing employee privacy and personal use of their devices can also mitigate potential risks," says Christina D. Frangiosa, an attorney at Semanoff Ormsby Greenberg & Torchia, LLC.

Smart Business spoke with Frangiosa about BYOD policies and the importance of implementing security protocols.

How can companies secure their data?

Companies should require employees to agree not to disclose confidential company information to any unauthorized persons using their devices. Employees must use best efforts to protect company data accessible on their devices from misuse, including applying passwords to their devices, relying on randomly-generated company passwords to access confidential company data, installing any company-required security software as a condition of obtaining access, and perhaps installing mobile device management software to allow the company to update access rights and secure company data in the event of a potential breach.

How should ownership of company data be communicated?

Identify the company's basic claim to confidential data from the outset so that it's clear what scope of protection the company claims. This identification can also remind employees that their limited access rights to company data can be withdrawn if they do not take precautions against misuse of their devices, or for other reasons company policies may outline.

How should loss or theft be handled?

Employees should be required to report a loss or theft of their devices immediately so that company-generated passwords can be changed, minimizing the potential exposure for a data breach. If the company has a mobile device management system in place, it may be able to remotely remove company data from an employee-owned device. The company should not remotely wipe the whole device, including the employee's personal data, without the employee's express written consent. But if a device is truly lost or stolen, the employee may grant such consent quickly. If an employee leaves the company, remotely wiping the whole device should not be automatic; express written consent is still required.

Is data stored on an employee's personal device discoverable in litigation?

Maybe. If companies permit employees to conduct company business using their own devices, relevant communications about company business stored on these personal devices may be discoverable if the company gets sued, and the company may have to produce them to avoid sanctions. Provide training to employees to be sure they understand this requirement. Begin these conversations as early as possible after the employee is hired and obtain their written agreement to cooperate with the company if such an event occurs.

Companies may also need to inspect employee devices periodically to ensure that required security protocols have been installed, but should not exceed authorized access given to a device or access clearly personal areas of the device. Avoid the temptation to check an employee's private email stored on another server. The Stored Communications Act and/or the Computer Fraud and Abuse Act may prohibit such access, and violations may expose the company to liability.

Who pays for device upgrades and service?

If the objective is to save money on the front end by permitting BYOD, then the company should clearly disclose that it does not provide technical support or device replacement at the company's expense. BYOD devices are entirely within the control of the employee. The company's only concerns should be with the manner in which these employee devices can access, store and/or share company data and company secrets. ●