September 9, 2013

Is BYOD Right For Your Workplace?

Twenty-four hour, world-wide instant access to personal email, contacts, calendar, and bank account information? Using a small device like a mobile smart phone? No big deal in 2013. Many employers supply workers with these devices to create constant connectivity to the work environment.

An increasing number of employers have instituted a "bring your own device" (BYOD) policy. Those employers encourage employees to use their own devices—such as tablets, smart phones, and laptops—to perform work. Employees can connect their personal equipment to company servers from anywhere in the world, allowing immediate communication and access to business information at any time.

Of course, a BYOD culture is not right for every employer. Cost-savings and employee flexibility may be outweighed by business concerns, such as regulatory compliance and trade secret and data protection risks.

While many employers have policies that focus on the appropriate use of corporate data on company-issued devices, existing policies may not effectively address the blurring of lines between company and personal equipment used for work purposes. Employers should consider implementing a personal device/BYOD policy – whether or not they encourage employees to BYOD – to ensure that employees understand the rules when it comes to using personal devices on the job. Important considerations include:

- Regulatory coverage. If the employer operates in a highly regulated industry (such as banking or health care), BYOD may not be appropriate or may even be prohibited.
- Scope. The BYOD policy presumably would apply to working and nonworking hours, and on and off company premises, but the policy must specify.
- Compliance. The policy should determine how the company plans to track hours worked for hourly workers, and remind employees of the need to comply with harassment and discrimination policies.
- Acceptable Use. The employer should specify who is allowed to use the device, for what purposes, and in what manner. The policy also should address permitted configurations, downloads, and storage of business email/attachments/documents.
- Expectation of Privacy. Presumably the company controls and owns all information on the device that is created or accessed in connection with work. If so, the employer must decide how to monitor, search, and control the device without unduly intruding into purely personal information.
- Security Requirements. The employer needs to determine requirements for password protection, encryption, updating of software, and the use of remote lock and wipe functionality.

AUTHORS:
Steve Peltin

RELATED SERVICES:
Employment & Labor

September 9, 2013

Is BYOD Right For Your Workplace?

- Storage. The policy should specify how data is stored on the device, how the data is backed up to company servers, and how the employer will map the data created, accessed or stored on the device.
- Regulations for Security Breach. The employer should identify the notification protocol in the instance of potential data loss or damage.
- Separation. The policy should establish a process for protection of company data at termination of employment.
- Litigation Hold. When required to preserve electronic documents in the course of a lawsuit, the employer will need to determine how to capture communications and data on personal devices.

Developing an effective BYOD policy requires collaboration among various groups, including HR, IT and business units. An effective policy will address employer needs, likely employee use patterns, and steps to protect company data. If employers believe BYOD is appropriate, they should implement a policy, communicate the policy to employees, and train and enforce compliance with the policy.

If you have questions about BYOD policies in the workplace, please contact the Employment & Labor group at Foster Pepper.

For more information about Foster Pepper or to register for other firm communications, visit www.foster.com.