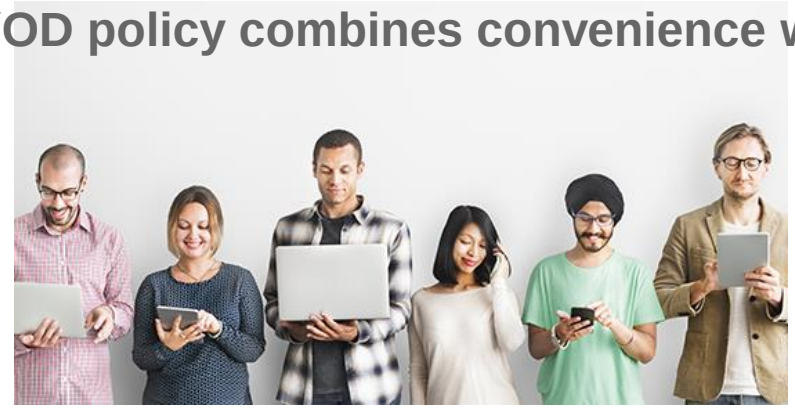
A strong BYOD policy combines convenience with security



It's easy to understand why more and more businesses are taking a "bring your own device" (BYOD) approach to the smartphones, tablets and laptops many employees rely on to do their jobs. BYOD can boost employee efficiency and satisfaction, often while reducing a company's IT costs. But the approach isn't without risk for both you and your staff. So, it's highly advisable to create a strong formal policy that combines convenience with security.

Primary concerns

As an employer, your primary concern with BYOD is no doubt the inevitable security risks that arise when your networks are accessible to personal devices that could be stolen, lost or hacked. But you also must think about various legal compliance issues, such as electronic document retention for litigation purposes or liability for overtime pay when nonexempt employees use their devices to work outside of normal hours.

For employees, the main worry comes down to privacy. Will you, their employer, have access to personal information, photos and other non-work-related data on the device? Could an employee lose all of that if you're forced to "wipe" the device because it's been lost or stolen, or when the employee leaves your company?

Important obligations

A BYOD policy must address these and other issues. Each company's individual circumstances will determine the final details, but most employers should, at minimum, require employees to sign an acknowledgment of their obligations to:

- Use strong passwords and automatic lock-outs after periods of inactivity,
- Immediately report lost or stolen devices,
- Install mandated antivirus software and other protective measures,
- Regularly back up their devices,
- Keep apps and operating systems up to date, and
- Encrypt their devices.

The policy also should prohibit the use of public wi-fi networks or require employees to log in through a secure virtual private network when connecting via public wi-fi. You may want to forbid certain apps, too. In addition, you need to spell out your rights to access, monitor and delete data on employees' devices — including the types of data you can access and under which conditions. In particular, explain your wiping procedures and the steps employees can take to protect their personal information from permanent erasure.

Protection now - Nearly everyone who works for your company likely has a smartphone at this point. As such devices integrate themselves ever more deeply into our daily lives, it's only natural that they'll affect our jobs. Establishing a BYOD policy now can help prevent costly mistakes and potential litigation down the road. We can provide further information.