Technology & Innovation Focus

Expert Insight

Employers must define their BYOD policies

By Heinan Landa

Having myriad technology devices in the office creates a bit of chaos, which is especially concerning – and risky – when you think about your company's data.

It also raises a multitude of questions that you must be prepared to answer and provide a corporate policy to address.

BYOD, or Bring Your Own Device, is an information technology strategy that encourages and supports employees bringing in their own personal devices, and it sets out policies and specifications regarding these devices. At the bare minimum, your corporate BYOD policy should do the following:

Define and specify. You must decide which devices you are going to support. All mobile devices? Just cellphones? Just tablets? Then you must specify what versions and levels of devices your company will support – for example, all cellphones that run iPhone operating system 6.0 or greater or Android Ice Cream Sandwiches operating systems or greater. Stay current; you don't want to encourage employees to bring in old devices with outdated operating systems that can cause headaches and security problems for your information technology team.

Address the apps. Clearly state which apps will be supported. Will you only support email functionality? Or will you support calendaring, Word, PDF readers and an entire office suite? Be specific.

Determine payment. This section needs to define who will be paying for the device, work apps and ongoing usage charges. Employees need to understand which charges they are responsible for paying.

Protect/secure data. Explicitly lay out the types of protection and security you will be requiring on these devices. This should include things such as anti-malware programs, be they for Windows and Android devices, and restrictions on downloading company documents. Will there be certain anti-virus, anti-spam and anti-malware that your organization will provide and support? Will there be rules against downloading company documents? Will you be limiting network or application access to enhance security?

Have action plans if the employee leaves or is terminated. Your BYOD policy must address what happens when an employee leaves or is terminated from the company. It must also include actions that will be taken if a device is lost. It is imperative that corporations retain the right to remotely wipe all data from a device in any of these scenarios.

Provide access/collaboration. This section should address how corporate information will be shared on these devices. Will you create access to a corporate DropBox account, or will access be more sophisticated and extensive – allowing employees to access their desktop from these mobile devices, for instance? If you leave this up to the individual, then you will find that everyone is accessing data differently, and you will have some data chaos on your hands, which is difficult to remedy.

At the end of the day, BYOD is more than just a policy; it is a shift in corporate culture. If your organization is one that requires personal mobile access for maximum productivity and you are willing to invest the IT support dollars that inevitably come with a strong BYOD policy, then go for it. If, on the other hand, you are leading a high-security organization or your company's industry is highly regulated and requires multiple levels of compliance, a BYOD environment might not right for you.

It is important to remember that the greater the variety of devices you allow onto your organization's network, the higher your risk for data loss. BYOD policies must be thorough, comprehensive and accompanied by multiple training activities to ensure that both employees and corporate executives understand the benefits and risks.

Heinan Landa is CEO of Optimal Networks Inc., a Rockville computer and network support services company.