WHAT SHOULD AN **EFFECTIVE** BYOD POLICY CONTAIN

BY HEINAN LANDA

Bring Your Own Device (or BYOD) is an IT strategy that encourages and supports employees bringing in their personal devices and sets out policies and specifications regarding these devices. Having myriad devices creates a bit of chaos, which is especially concerning (and risky) when thinking 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.

At the bare minimum, your corporate BYOD policy should contain the following:

- **Define and Specify**: You must decide which devices you are going to support. All mobile devices? Just cell phones? Just tablets? Then, you must specify what versions and levels of devices your company will support. For example, all cell phones that run iOS 6.0 or greater or Android Ice Cream Sandwich 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 IT team.
- **Password Rules**: Your BYOD policy must outline password specifications for your users. Will the device rotate passwords after a certain period? What is the minimum number of characters required for the password and are you regulating a certain password construction? Will the device lock after a number of unauthorized attempts to access data?
- **Address the Apps**: Clearly state which apps will be supported. Will you only be supporting email functionality? Or will you be supporting calendaring, Word, PDF readers and an entire office suite? Be specific.
- **Payment**: This section needs to define who will be paying for the device, work apps and ongoing usage charges. Employees need to understand for which charges they are responsible.
- **Data Protection/Security**: Explicitly lay out the types of protection and security you will be requiring on these devices – this should include everything from anti-malware programs (on Windows and Android devices) to 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?
- **Employee Leaves or Terminations**: Your BYOD policy must address what happens when an employee leaves – or is terminated from – the firm. It must also include actions that will be taken if a device is lost. It is imperative that companies retain the right to remotely wipe all data from a device in any of these scenarios. In addition to leaving or being terminated, clearly state that the employee's device will be remotely wiped if the employee loses the device, a data or policy breach has been detected, or if an incorrect password is typed in more than a certain number of consecutive times.
- **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 (e.g., allowing employees to access their desktop from these mobile devices)? 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.
- **Expectation of Privacy**: It should be noted that your organization respects the privacy of its employees, but that a device used for work will need to be accessed by multiple stakeholders. The privacy policy should note that any and all communications passing through the device (even personal ones) could be accessed and referred to at any time.
- **Liability**: Your organization's BYOD policy must contain a section on liability that protects the company from the loss of any of the user's data and from any service disruptions. In addition, note that you have the right to remove any supplied applications from the device as a result of a violation of the BYOD policy. In addition, your policy should include a statement about how users are expected to follow all safety laws, regulations, and common sense when using their smartphones (i.e., no texting while driving).

LAST WORD

At the end of the day, BYOD is more than just a policy; it is a shift in corporate culture. 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 trainings to ensure that staff, associates and your firm's executives understand the benefits and risks.

About the author

Heinan Landa is CEO of Optimal Networks, a company that provides comprehensive computer and network support services including full or partial IT management outsourcing, back-up and disaster recovery, cloud computing, and technolo gy consulting services to law firms, associations and small- to mid-sized businesses. For more, visit *www.optimalnetworks.com.*