BYOD ASAP

Posted At : November 25, 2014 8:50 AM | Posted By : Admin
Related Categories: BYOD, Hewlett Packard

The reality of bring your own device (BYOD) is unavoidable. If your organization has yet to implement a BYOD strategy, you can take several steps to get started. But first, know that the question is no longer whether you will support mobile devices. Instead, it's how do we secure and manage these devices in a user-friendly way?

A **Forbes Insights and Google survey** of U.S. business executives found that by 2016 more than half of leaders expect to use mobile devices instead of PCs as their primary business platform. By 2020, **HP estimates** that each professional in the workplace will use more than six mobile devices.

A well-crafted BYOD strategy can facilitate increased employee productivity and engagement in an era of mobile-first behavior that has begun to blur the lines between work demands and personal usage. As you and your team develop the appropriate strategy for your organization, realize that there is no “one-size-fits-all” solution to this endeavor.

“It is important to remember that BYOD itself is not a technology,” **says Dragana Beara**, Senior Solutions Marketing Manager, HP Networking Global Marketing. “It’s a behavior. The challenge that organizations currently face is deciding how to respond to this behavior and the technology solutions they need to enable that response.”

Your business is unique, and the BYOD strategy it needs to manage mobile devices should be as well.

Forming a strategy
“Mobility itself can be described as providing universal access to people, apps, and data. However, most existing networks are completely unprepared to deliver services in this way,” Beara says. “The ultimate aim of BYOD—driving productivity and engagement—can only be fully realized when the behavior is embraced and your infrastructure has been transformed to accommodate it.”

Your team should consider and resolve a series of questions that will guide your development of a BYOD strategy:

- **What devices will be permitted?** In an age of tablets, work phones, personal phones, and more, your policy should outline which devices you will support and which you will not.
- **What will your security policy include?** Should you require employees to use lock screens? Will you allow BYOD devices to be used by others outside of your organization? Consider all potential security threats as you craft this portion of your policy.
- **What will your service policy encompass?** As employees use their personal devices more for work purposes, they must also be clear about what technical issues your company will or

will not help resolve.

- **What apps will you allow, and which will you prohibit?** Will you allow social media apps? Will employees be allowed to use replacement email or VPN clients? You may wish to limit the number of apps that you allow as well.
- **How will you determine and track what data the business owns?** Know what data and apps you own in the event of a stolen or lost device, which may need to be wiped clean.
- **What will your acceptable use policy include?** If an employee sends out inappropriate material over your VPN, will there be any consequences? Outlining what is acceptable or prohibited provides your organization with a much-needed safeguard.
- **How will you treat mobile devices when an employee leaves a company?** Outlining the process to take when employees leave the company—with their BYOD-covered devices—is necessary to prevent security breaches and counter the risk of information falling into the wrong hands.

Don’t forget to audit your BYOD policy once you have implemented it. Also, we recommend you incorporate a zero-tolerance policy for noncompliance, to ensure everyone adheres to your new strategy.