SERVICE BRIEF

Understanding Bring Your Own Device

Measures in response to personal device access are paramount to network security.

Why You May Consider BYOD

This strategy provides definite benefits, if carefully managed.

In a world where seemingly everyone has a device that they bring everywhere, how can you make this trend work for your business while keeping your IT infrastructure from being infiltrated by malicious entities? By instituting a conscientious and thorough Bring Your Own Device (BYOD) strategy, your company can make your staff's devices work for your company.

Most business owners would agree that their employees already bring their smartphones to work, and will continue to do so whether your company policy allows them to or not. According to a study by Microsoft, over 67% of employees at surveyed companies bring their devices to work, regardless of their company's policy.

Weighing The Benefits of BYOD

Based on the statistics, BYOD may seem to be a no-brainer, but there are other variables to consider.

For instance, a major point of contention between network administrators and employees is that many mobile device management strategies include an option to wipe the device of a user that has left the company. While this is something that the user would have to agree to, most users would rather remove the company data voluntarily than have their personal device wiped clean. For reasons like this, BYOD is not a cut and dry matter, even for companies that have been doing it since before it was known as BYOD.

The first consideration you should have is whether or not the additional mobility would be of any benefit for your organization. The ability to reach beyond your network and still access all the work-related material can be an indispensable factor for the modern employee and has to be a consideration for any business owner looking to expand his or her business.

Conversely, as a business owner you'll also need to understand what threats the threats that are inherent by allowing foreign devices to access your network, as well as the issues that come with allowing your data to be accessible on other networks. With sensitive data breaches costing companies thousands of dollars, can your company sustain itself if you were put in that unenviable position? At Edit Technology Solutions, we've designed and implemented mobile device management solutions for companies to improve their portability and use their advanced mobility to enhance production.

Defining Acceptable Use

This strategy provides definite benefits, if carefully managed.

Another variable you will have to consider is that of an Acceptable Use Policy that governs what content is available to people on your network. This policy is created with the best interest of the organization in mind, implemented by the network administrator, and policed to the extent required by your organization. In this policy you are able to set forth what is off limits to the end users.

The consideration of these variables will go a long way toward concocting a BYOD policy that both fits your organization and ensures that the security of your data isn't available to be compromised.

Key Determinations

In order to design a BYOD policy that works for your company, there are a few points that must first be established:

- What are you trying to protect?
- How much access do your employees have to that which you are trying to protect?
- What reaction should there be when your BYOD policy's protocols have to be enacted?

Variables to address

1. Specify which devices will be permitted on the network.

2. Establish static and comprehensive security strategy.

3. Define how foreign devices can access data on the network.

4. Ensure staff knows who owns what on the mobile device.

5. Make a decision on what kind of use to ban on foreign devices.

6. Combine your BYOD strategy with your acceptable use strategy.

7. Create a strategy to quickly and securely onboard and remove users.

Get proactive and call us TODAY!

(866)282-2810 | www.etsinc.online | info@etsinc.online

Edit Technology Solutions, Inc.
3415 S. Sepulveda Blvd.
Suite 1100
Los Angeles, CA 90034