THE ROMAN CATHOLIC ARCHDIOCESE OF ATLANTA

INFORMATION TECHNOLOGY
ARCHDIOCESE OF ATLANTA

Creating a Policy for Bring Your Own Device (BYOD)

A 2016 Gartner survey shows that 39 percent of employees in the United States use their personal devices at work. That includes things like smartphones and tablets. By contrast, only 10 percent of employees report using devices issued to them by their employers.

Bring your own device (BYOD) has become even more popular since that report was released. Unfortunately, there isn't much information suggesting that companies have developed BYOD policies to protect themselves and their employees.

If you want to let your employees use their personal devices for work-related activities, then you should learn how to create a BYOD policy for your SMB.

Understand the potential threats of BYOD

You can't write an effective BYOD policy until you understand the potential threats of letting employees use their smartphones for work. Some of the biggest security threats of BYOD include:

- Malicious websites and apps that compromise your network security
- Lost devices that give unauthorized users access to sensitive information like email contacts, phone numbers, contracts and any data stored on your company's network and apps
- Employees who don't understand the importance of keeping personal information separate from work data and apps
- Jailbroken (rooted) smartphones that no longer include the manufacturer's security features

Since BYOD can put your business's security at risk, it's not a bad idea to have a professional perform a security risk assessment that will uncover your current vulnerabilities.

Know the benefits of BYOD

Now that you know the potential threats of BYOD, you might wonder why businesses allow it.

When done correctly, BYOD can offer your business several benefits. A lot of companies feel that the benefits outweigh the risks. Besides, they know that creating an effective BYOD policy will mitigate some of those risks.

Benefits that you can expect from adopting a good BYOD policy include:

- Increased productivity
- Saving money by transferring the cost of mobile devices to your employees
- Making remote workdays possible, which will appeal to Millennial workers who prefer flexible schedules

June 2024

Writing an effective, secure BYOD policy

If you decide that you want to take advantage of BYOD's benefits, then you will need to write a BYOD policy that protects your security, business and employees. Follow these four tips to make your BYOD as effective as possible.

1. **Use straightforward language**

People can only follow policies that they understand. Use straightforward language and avoid technical jargon so your employees will know how to follow your BYOD policies.

2. **Authorize certain apps for business use**

BYOD can make it easier for employees to use shadow IT, such as apps that you haven't authorized. Unauthorized apps could contain vulnerabilities that give hackers access to your network. Choose cloud services that your employees can use and ask them to avoid apps that haven't been reviewed.

3. **Require anti-malware software**

If your employees are going to connect to your network, then you need to make sure they use devices with reliable anti-malware software. Choose an option that matches your business needs. If the software costs money, pay for it. You don't want someone to put your security at risk over a few dollars.

4. **Educate your employees**

Your BYOD policy should include an educational requirement to make sure your employees know how to use the internet, apps and other tools safely. For instance, they should know the warning signs of a phishing attempt and how to spot a fake website.

BYOD comes with a lot of benefits, but you have to take some precautions to make sure you keep your business, and employees secure.