Expand Your Workflow Potential By Safely Implementing BYOD

EACH DEVICE THAT CONNECTS TO YOUR COMPANY'S NETWORK OPENS UP **A NEW ENTRYWAY FOR HACKERS' POTENTIALLY ATTACKS.**

Businesses are always looking for ways to modernize and bring their workflow up to speed with the latest industry demands. One trend that addresses this need and is sweeping across enterprises all over the nation is the increasing acceptance of mobile devices in the workforce, also known as BYOD.

BYOD, or "bring your own devices", refers to the company policy of giving employees the freedom to use their own hardware for work purposes. These devices might include cellular phones, notebook computers, or tablets.

Having all of these device options brings great benefits to businesses, such as flexibility and lower costs, but it also brings about more risks. Each device that connects to your company's network opens up a new entryway for hackers to potentially attack.

GB Tech has a solution to these threats. Our enterprise mobility management, or EMM, services prevent security breaches and attacks via devices connected to a company with a BYOD policy, allowing you to work without worry and utilize all of the benefits your devices provide.

Benefits of BYOD

There are many benefits that come with a mobile work environment. With the freedom to work from anywhere, anytime, on any device:

- **Access emails, shared files, applications, and network data faster**
- **Complete tasks in less time**
- **Collaborate more effectively**
- **Work more efficiently with company data readily available**
- **Increase overall flexibility**
- **Reducing costs by reducing the amount of devices needed to be purchased**
- **Expand your network by allowing for remote work from various locations, making it easy to get work done whether you're at home or on a trip**
- **Contribute to employee satisfaction**

THE MAJORITY OF EMPLOYEES WHO OWN A SMARTPHONE OR TABLET USE IT TO ACCESS CORPORATE DATA.

Entrepreneur magazine even says that BYOD policies can boost employee productivity. Clearly, BYOD is a great technique for businesses to implement, but it's very important they do it safely.

How to Ensure the Security of Company Data

The majority of employees who own a smartphone or tablet use it to access corporate data. This brings up a major concern because all of these endpoint devices open up entry points for hackers and other cyber threats. This is why safety measures and precautions are absolutely necessary to make certain that company information does not fall into the wrong hands.

With EMM services from GB Tech, we've got that covered. Our EMM team is focused on analyzing and managing your processes, technologies, wireless networks, and any other mobile computing device that connects to your network and your valuable data. We will provide safety by implementing processes such as data encryption, personal firewall, application control, and network access control onto cellular phones, tablets and laptops.

We also have a process called containerization to further protect your data. Containerization is when we contain your corporate and personal data in separate, protected areas on your endpoints. Each type of data will have its own operating environment this way, significantly reducing the chance of a mixup error.

Some other ways EMM from GB Tech will securely manage your mobile devices include:

Restrictions

Camera use, screen capture, and cloud backup may be restricted to prevent vital information and data from being compromised.

Content Management

Email scams, websites that use flash, and download sites are some of the most dangerous places on the web. Access to these websites can be unauthorized. Mobile device management and surveillance software may feature alerts once these threats are accessed.

Security Codes and Credentials

Hacking is not the number one cause of security breaches. In fact, it is the loss or theft of mobile devices that account for 15.3% of security breaches. The need for passwords and biometrics for added security is irrefutable. A data breach can easily be prevented when access is restricted from unauthorized personnel.

Standards Compliance

We can implement standards for use of devices. The use of jailbroken or unlocked phones and routed devices may have their access to the network denied, since it has been known that they are prone to malware intrusions. Some operating systems may be preferable to others, but most EMM software, such as IBM's MaaS360, is compatible with Android, iOS, BlackBerry, Symbian, and other common systems.

Centralized Management

When you trust us with securing your mobile devices, we will control enrollment and oversee the mobile devices of your employees. With this, we can see if the employee complies with company standards, whether the employee has enabled passcodes, whether they have accessed unauthorized websites and if restricted features are used. GB Tech offers a feature-packed MDM from IBM that covers all of these aspects.

Damage Limitation

In the event of a lost or stolen device, Maas360 MDM software allows the administrator to completely wipe all data or selectively erase only company data. This is an extremely valuable feature for those devices that are stolen.

Embrace the Mobile Office Movement Today

Incorporating mobile devices into your business will improve your productivity in unprecedented ways. But you need to make sure you do it securely. When you come to us for secure mobile device management, we will reduce the risk and complexity of managing all those devices across your network. All you have to do is just sit back and benefit from content collaboration and secure access to corporate resources anywhere, anytime.

GB Tech is 1 of only 3 companies in Houston that is accredited by IBM for the MaaS360 MDM software. We have done extensive research, and we are dedicated to only providing the best for our clients. Get in touch to get started.

GB TECH
Information Technology

2200 Space Park Drive
Suite 400
Houston, TX. 77058

(281) 957-7550
www.gbtech.net