computer dimensions
Business IT Solutions

Tech Tips

August 2016 www.computerdimensions.net

Welcome...

...to Tech Tips. Insider Tips and Secrets to Get the MOST Out of Your Computer.

BYOD (Bring Your Own Device) Data Concerns
(And How To Overcome Them!)

Are your employees putting your business at risk when it comes to BYOD? Although BYOD offers greater flexibility and increases productivity, there are a number of security risks associated with it.

Compliance Issues – If your employee had access to information covered by any number of regulations, your company could be subject to stiff penalties. One employer we know of wound up with a $100,000 fine.

Data Security – Sensitive company data in the wrong hands could spell disaster. Access to your network, secure sites, proprietary files, work-related e-mails and intellectual property may now be out of your control. Company policy regarding BYOD (bring your own device) and data loss need to be clearly stated and agreed to up-front. *Here are six smart measures you can take right now to prepare for a BYOD model:*

1. Install a mobile device management (MDM) system on any employee device to be used at work. This software can create a virtual wall separating work data from personal. It facilitates any security measures you wish to impose. And to protect employee privacy, it can limit company access to work data only.

2. Determine which devices will be allowed and which types of company data people may access from them.

3. Require that employees agree with an Acceptable Use Policy before they connect to your network. Make sure these include notice as to conditions in which company data may be "wiped" – i.e., destroyed. Also include specific policies regarding device inspection and removal of company records.

4. Put strong data protection practices in place. Require use of hard-to-crack passwords and auto-locking after periods of inactivity. Establish protocols for reporting lost or stolen devices. Mandate antivirus and other protective software as well as regular backups.

5. Designate IT support to authorize access to software and critical data. They will be your main point of contact for questions about BYOD policy and practices. It might also work well to distribute a resource page or FAQ document to your employees.

6. Establish a standard protocol for what to do when a device is lost or stolen. Both Android and iOS phones have features that allow device owners to locate, lock and/or "wipe" all data on their phones. Make sure your policy requires that these features are set up in advance. Then, when a device is lost or stolen, your employee can be instructed to take appropriate action according to your protocol in order to protect company data.

Want Help In Implementing A BYOD Policy
Give us a call at (520) 743-7554