Alpha Tech

"News about IT Technologies that can help your business prosper"

Millbury, MA

Do You Allow Your Employees To Use Their Own Mobile Devices For Work?

The evolution of personal mobile devices and the rise of how necessary they are to business success these days are forcing many small business owners to make a choice - "Bring Your Own Device" (BYOD) vs. "Corporate Owned, Personally Enabled" (COPE).

The Typical Solution - BYOD.

According to the CDW 2012 Small Business Mobility Report, 89% of small-business employees use their personal mobile devices for work. But the headache involved here is how do you support and secure all of these devices? The scary thing is that most small businesses don't even try! The CDW survey found that only 1 in 5 small businesses have deployed (or plan to deploy) any systems for managing and securing employees' personal devices.

The Alternative - Is COPE Any Better?

A minority of small businesses has implemented a Corporate Owned, Personally Enabled ("COPE") policy instead. They buy their employees' mobile devices, secure them, and then let employees load additional personal applications that they want or need. And the employers control what types of apps can be added too. And the "personally enabled" aspect of COPE allows employees to choose the company-approved device they prefer while permitting them to use it both personally and professionally. COPE is certainly more controlled and secure, but for a business with a limited budget, buying devices for every employee can add up pretty quick. If you go the COPE route and are large enough to buy in volume, you can likely negotiate substantial discounts.

Security Concerns With BYOD.

If you have client information that must be kept secure or other industry specific regulations regarding the security of client data, then COPE is likely your best approach. It takes out any gray area of whose data is whose. Plus there is a certain comfort level in being able to recover or confiscate any device for any reason at any time to protect your company without any worries of device ownership. Whichever way you go, you can use a Mobile Device Management (MDM) solution to manage and protect those devices. If doing BYOD, you can make the MDM installation a pre-requisite for using a personal device to access company data.

Free Mobile Device Policy Consultation

Which mobile device policy is appropriate for your business? We'll help you build a solid mobile device management system that protects your organization from a number of risks. During this meeting:

- We'll match up your business objectives and your specific risk tolerance with what you want to enable your employees to do and how you want them to work.
- We'll review your current mobile device policy against our 11-point mobile device policy checklist. Skipping any of the 11 "must-haves" could lead to big problems.
- We'll review your "Locks on the doors" of your devices. A written policy is not enough! We'll review 4 critical areas of your mobile device management system too often missed by small businesses.

Struggling to figure out which option is best for your business? Our FREE Mobile Device Policy Consultation ($297 value) helps point you in the right direction for your business.

Fast-Action Response Form

Your Name: _____

Title: _____

Company: _____

Address: _____

City, State, Zip: _____

Phone: _____

E-mail Address: _____

Tell us about your situation: _____

_____

_____

_____

Fax This Completed Form To: (508) 519-3051

Alpha NetSolutions, Inc.
3 Silver Fox Dr, Fl 1, Millbury, MA 01527
Phone: 508-471-3155