Kelley Technology Group
MOBILITY SOLVED

6 Steps to Create a Mobile Device Policy

The statistics on mobile devices these days is utterly phenomenal when we consider that just ten years ago, owning a mobile device of any sort was less the norm and more an option for only the most technologically-advanced mindsets. While very few probably even need to see the real statistics, understanding them can definitely help when creating a mobile device policy. Currently, studies by various organizations such as cisco and pewinternet have shown that:

- 87% of adults in America own a mobile cell phone
- 45% own a Smartphone
- In 2013, the number of mobile devices will officially exceed the population of earth

With impressive statistics like this, you do not want to be left out in the cold with a hastily arranged or ineffective mobile device policy for your business or organization. Here are six ways to create the perfect policy for you.

1. Keep Concise Goals in Mind

Know what you want, make a viable plan that will enable you to reach that goal, and follow through with dedication and determination. Your ultimate goal as a supplier is to empower your consumers and encourage them to utilize their mobile devices for tasks whenever possible. While it is understandable to protect your own investment by limiting bandwidth hogging networks such as Netflix or Youtube, you will still want to provide your employees with the access they need to do business, shop or other tasks that many can and will do on desktops or laptops if mobile navigation is difficult or too slow.

2. Understand that in the Mobile World, One Size Does Not Fit All

While you want your employees to have mobile access so that they can be within reach and able to remain productive when traveling on the train, or waiting on long lines, or even have the ability to communicate socially during conventions and meetings, you do not want to supply so much access that you expose your own company to unnecessary risks with an unprotected network. It is up to you to find the happy medium and a proper balance that will allow you to provide appropriate access to staff who need it while not opening up that possibility to those who shouldn't be privy to network data. The closer your policy comes to what staff requires to function, the easier it will be to get them to apply the proper protocols that they can to ensure network security.

3. Ask for Feedback from All Departments

Even the staff that is not directly involved with your mobile network and development should be given consideration when proceeding with any IT project. Make sure all leaders and management are on the same page and understand the policies you plan to enforce on mobile devices. Explain to all staff the benefit and the privilege of their access while also making certain they understand how easily the privilege can be abused by employees and outsiders alike. Encourage them to protect their own mobile access by helping management and administrators understand when and where there may be an issue with the abuse of network access. Before you are done, ask your staff what they think you can do in development as well as a team to protect this particular investment. Many heads are always better than one and brainstorming sessions like these often provide viable answers from the strangest places. Give everyone a chance to speak up.

4. Incentive and Responsibility

If your IT staff is planning to manage personally owned devices you will in essence, also be enforcing your business's security policies on them. If you expect employees to allow this, you will likely need to provide them with an incentive to encourage this act of accession. While you should definitely get users to understand the responsibility that can come along with using their own mobile device for work, understanding the need to protect company data is critical. If your business network houses seriously confidential information such as a health or law practice might, make sure your staff understands that in cases of lost devices, all onboard data may be deleted remotely. Supply the upside. Will you allow your staff to select the mobile device of their choice? Pay for their current contract? Regardless of what incentive you select, you will need to select one that benefits your staff inclusively and fairly. Keep the incentives going by updating your staff with trending new mobile devices when at all possible.

5. Be Prepared to Be the Enforcer

Once you have an established policy and have taken all measures necessary to share those with relevant staff, it will be time to enforce any and all of your rules, even if you have to make an example of your first detractor. While there is software that will enable administrators to monitor activities across mobile devices, in most cases, unfortunately, a breech in guidelines is often noticed first because of device failure resulting from malware or malicious content that staff should have likely never been utilizing in the first place. When a policy is broken, have set consequences in line and

use them every time, with all employees regardless of their status in the workplace. You can always go one further and make public notice of those who have had their mobile access restricted and why. There are endless creative ways to supply the proper encouragement as well as understandable punishments for serious infractions.

6. Education is Key

While the organization, planning and development of the mobile device policy is critical to the long term success of utilizing your business's network in this fashion, it is equally, if not more important to educate, instruct and support the staff you have that will function at work and away on your business network. Education is key and it is the responsibility of upper management and every member on your C-List to participate in the program on an administrative level as well as that of the level of hourly employees to ensure that everyone from top-to-bottom leads by example in this critical element of business management.