How to Establish a Bring-Your-Own-Device Program

It is estimated that the number of smartphones in use across the world will reach 2 billion by the end of 2015. Also, according to Forrester Research, 53% of employees use their own devices at work and this trend can add as many as 240 productivity hours a year for each mobile employee. Therefore, if you haven't already been encouraged to establish a program to allow personal employee-devices to access corporate email, calendar and contact systems, this should be a focus for the New Year.

Accepting the trend of employee owned devices is the easy part. The challenges to these types of programs are the keys to developing a solid Bring-Your-Own-Device (BYOD) policy and how best to implement the program into your business. To help you make the most of employee owned devices, these are seven core ideas that should be part of any good BYOD program. Each idea comes with many important questions to ask yourself, your IT employees and your executive team while the policy is being developed.

1. Specify What Devices Are Permitted

The mobile phone market has exploded over the last few years and, unlike the old days where only BlackBerry was used for work, there are a lot more device choices, from iOS-based phones and tablets, Android handhelds and tablets to Research in Motion's Playbook and many others. Therefore, it is extremely important to decide what you mean when you say "bring your own device". Make it clear to your employees who are interested in BYOD which devices you will support and which ones you won't.

2. Establish a Firm Security Policy for all Devices

Passwords and lock screens are often overlooked on personal devices because of their believed inconvenience to the access of content and functionality of the device. However, if your business is looking to implement a BYOD program, security is important for safeguarding your business and the sensitive information employees will have access to on their own devices. If your users want to use their devices with your system, they should comply with password requirements. Remember, strong, alphanumeric passwords are important for protecting the integrity of your network. Check with your messaging administrators to see what device security policies you can reliably enforce with your software.

3. Define a Clear Service Policy

When implementing a BYOD program, it is important to set boundaries and for your employees to understand them. The following are some important questions to help set these boundaries:

What level of support will be available for initial connections to your network from personally-owned devices?

What kind of support will IT representatives provide for broken devices?

What kind of support will IT representatives provide for applications installed on personal devices?

Will Help Desk be limited to problems with email, calendaring and other personal information management-type applications?

What if a personal application is preventing access to the applications designated for work, which are supported? What happens then?

Will your support be a "wipe and reconfigure" operation?

Will loaner devices be provided if a phone or tablet is being serviced?

BYOD, But Don't Drop It

Most companies that have a BYOD program require employees to handle repairs on their devices.

If an employee's personal device breaks, who is responsible for fixing it?
82%: Employees are responsible for having their devices fixed themselves and for paying for the repair.

12%: Employees are responsible for having their devices fixed themselves and our organization pays for the repair.

5%: Our organization assumes responsibility for fixing employee-owned devices.

2%: Not sure.

Source: CIO.com survey of 131 companies with BYOD programs, August 2011; percentages do not add to 100 due to rounding.

4. Make it Clear Who Owns What Apps and Data

While it might be clear cut to you that your company owns the personal information stored on your employees devices, it becomes problematic when devices are lost or stolen and are required to be wiped. When a device is wiped, all content is erased including the personal pictures, music and applications that your employee has paid for. Sometimes the replacement of these items is impossible. Therefore, it is important to make it clear that you assert the right to wipe devices brought onto the network under your plan, should the need arise. Additionally, guidance should be provided to employees about how they can secure their own content and back it up so it can be restored once their device is replaced.

5. Decide Which Apps will be Allowed or Banned

Deciding which applications are allowed or not is an important part of protecting the integrity of your network. Major considerations typically include any type of applications for social media browsing, replacement email applications and VPNs or other remote-access-software. The question to ask is whether users can download, install and use an application that presents security or legal risk on devices that have access to your sensitive business data.

Developing a clear methodology for backing up the user's personal information prior to an "exit wipe" is also another question to consider.

6. Integrate Your BYOD Program with your Acceptable Use Policy

If your business is on the ball, chances are that corporate-issued devices are already covered and treated like notebooks, desktop computers and other equipment that connects to your network. However, when you start dealing with personal devices, there begins to be doubt about what activities may or may not be permitted. Discussions about acceptable use policy are essential to make sure your business data is protected. The following are some questions to consider:

If you set up a VPN tunnel on an iPhone and then your employees post to Facebook, is this a violation?

What if your employees browse objectionable websites while on their device's VPN?

What if they transmit, inadvertently or not, inappropriate material over your network, even though they're using a device they own personally? What sanctions are there for such activity?

What monitoring strategies and tools are available to enforce such policies?

7. Set Up an Employee Exit Strategy

One of the biggest and most overlooked ideas is what will happen when employees with devices on your BYOD platform leave the company. How will removal of access tokens, email access, data and other applications and information be enforced when it is not as clear cut as asking the employee to turn in the device? In this case, many companies choose to rely on disabling email or synchronization access as part of the exit interview and HR checklists, while some choose to perform a wipe of the BYOD-enabled device as a mandatory part of the exit strategy. Developing a clear methodology for backing up the user's personal information prior to an "exit wipe" is also another question to consider.

Want more information about BYOD or help implementing your own program?

To learn more about Bring-Your-Own-Device programs and how they can benefit your business, please contact Intega IT at (613)260-1114 or by email at sales@intega.ca.