Personal Mobile Device Use in the Workplace: There Is A Way

James Hess

Davenport University

CAPS795

Dr. Deanne Cranford-Wesley

July 20, 2012
Abstract

Technology continues to become more compact and more versatile. Out of this technological advancement is continued improvement on mobile devices such as smartphones and tablets. This paper will discuss the issues and complications of correctly implementing the use of mobile devices while maintaining the integrity and security of company data. The new trend that is becoming a difficult hurdle for the corporate world as well as the I.T. department is called B.Y.O.D. or Bring Your Own Device. Although there are many pros with allowing these mobile devices into the organization, this paper will discuss the real issues that surround the implementation of personal devices in the workplace.

The author will discuss the I.T. concerns of implementing personal mobile devices. I.T. is tasked with ensuring that the information that is being used on a daily basis is easily accessible by those that need to access it, the data is readily available and most of all, that the data is secure. If the mobile device is being used in a healthcare facility that deals with confidential patient data, then the device also needs to meet HIPAA (The Health Insurance Portability and Accountability Act of 1996) Privacy and Security Rules.

With the introduction of personal mobile devices in the workplace, this task of securing data can become more difficult. The major question that needs to be answered is how to properly implement personal mobile devices in the work place while meeting the needs of the organization and without sacrificing the security that needs to be in place to prevent confidential data from being compromised.

To be able to achieve the goal, which is to be able to implement the personal mobile devices within a secure environment properly, the author will conduct a questionnaire to determine how other companies are handling this very same task in a multitude of fields, the
pitfalls of past implementations by other organizations, the types of security concerns that surround mobile devices and the software and tools that are readily available to help secure these devices from an I.T. standpoint. Once the research has been conducted, this paper will help guide others in implementing personal mobile devices securely and properly in their own company or organization and also help those organizations to embrace the use of personal mobile devices correctly.
# Table of Contents

Abstract ........................................................................................................................................... 2  
Introduction ..................................................................................................................................... 6  
Literature Review ............................................................................................................................ 7  
Types of Mobile Devices ............................................................................................................ 7  
   Smartphones ............................................................................................................................ 7  
      Android OS .......................................................................................................................... 8  
      iOS ...................................................................................................................................... 8  
      Windows Phone OS ............................................................................................................ 8  
      BlackBerry OS .................................................................................................................... 8  
   Netbooks and Laptops ............................................................................................................. 9  
      Apple OS ............................................................................................................................. 9  
      Microsoft Windows .......................................................................................................... 9  
      Linux Distributions ........................................................................................................... 10  
   Tablets ................................................................................................................................... 10  
Mobile Device Benefits .............................................................................................................. 11  
Security Concerns ....................................................................................................................... 12  
   Viruses and Malware ............................................................................................................ 12  
   Device Hacking ..................................................................................................................... 13  
   Lost or Stolen Devices .......................................................................................................... 14  
Compliances for Different Fields ............................................................................................... 14  
   HealthCare Organizations ................................................................................................. 15  
   Financial Institutions ......................................................................................................... 15  
   Government Agencies ....................................................................................................... 15  
   Private Corporations ........................................................................................................... 16  
Survey ....................................................................................................................................... 16  
Software Evaluation .................................................................................................................. 16  
   MaaS360 ............................................................................................................................... 17  
   Zenprise ................................................................................................................................. 20  
   Microsoft Exchange 2010 ................................................................................................. 20  
Methodology .............................................................................................................................. 21  
   Conduct Survey .................................................................................................................... 21  
   Develop Policies and Procedures ......................................................................................... 21  
   Develop Authorization Request Form .................................................................................. 22  
   Trial the Software ............................................................................................................... 22
Results ........................................................................................................................................... 22
Policies and Procedures ............................................................................................................ 23
Approval Request ..................................................................................................................... 23
Software Selection .................................................................................................................... 24
Applications .......................................................................................................................... 24
Device Security ..................................................................................................................... 25
Rooted Devices ..................................................................................................................... 25
Survey Results .......................................................................................................................... 25
Recommendations ......................................................................................................................... 29
Conclusion .................................................................................................................................... 30
References ..................................................................................................................................... 31
Appendices .................................................................................................................................... 34
Appendix A Survey .................................................................................................................. 34
Appendix B MaaS360 Mobile Device Management (MDM) .................................................. 46
Appendix C MaaS360 Laptop Management ............................................................................. 47
Appendix D Process of Developing Security Policies .............................................................. 48
Appendix E Intel Social Media Guidelines .............................................................................. 49
Appendix F Policy and Procedures Document Sample ............................................................ 50
Appendix G Personal Mobile Device Use Request Sample ..................................................... 52
Appendix H Fields of Employment .......................................................................................... 55
Appendix I Mobile Device Use Summary ................................................................................ 56
Appendix J Receives Company Email on the Device .............................................................. 57
Appendix K Users that Utilize a Pin Number or Password ...................................................... 58
Appendix L Devices Lost or Stolen .......................................................................................... 59
Appendix M Employers Allow the Use of Personal Mobile Devices for Work Purposes ...... 60
Appendix N Employers Have Policies and Procedures in Place for Personal Mobile Device Use ........................................................................................................................................... 61
Appendix O Employer Requires Users to Sign Documentation to Use Personal Devices ...... 62
Introduction

Mobile devices such as smartphones, tablets, netbooks and laptops have been making their way into the workplace as important productive work devices. Companies in the past have been supplying the devices to their employees for use on the road and in the office. Now more so than ever, employees are looking for permission from their companies to bring in their own personal devices that may not be supplied by their employers. However this can be a major security concern for the companies and the Information Technology (I.T.) department. The issue that needs to be addressed is if there is a way to allow users to bring in their personal devices and manage the security that is needed to have a successful implementation.

Anytime there is access to confidential data on any mobile device, there is a need to go through all of the scenarios of what could happen and how to handle the different situations. Allowing an employee access to the company data, their email and access to internal documents can be very beneficial to the employee while they travel or work in the office. The major concerns that need be addressed with the use of personal the mobile devices consist of the following:

- What happens if a personal mobile device is stolen, lost or hacked that may contain confidential client or company data?
- How does an organization’s I.T. department manage the personal mobile device?
- What types of policies or procedures need to be implemented to make sure that the owner of the personal mobile device knows the restrictions the will be in place to be able to access company data and systems?

Embracing personal mobile devices for company use can be beneficial for the employee and the employer. However, there have been many occasions where devices such as laptops and
other mobile devices have been lost or stolen. Just a couple of these examples, which will be discussed further in this paper, have been the Apple iPhone prototype being left in a bar (Potter, 2011) and the UK doctor that lost his laptop which contained confidential patient data of 1,147 patients (Leyden, 2011).

Is it possible to embrace personal mobile devices within a company and maintain the security needed for the company and client’s data? The research in this paper will discuss what is needed to make the implementation of personal mobile devices a possibility while maintaining the security that is needed.

**Literature Review**

**Types of Mobile Devices**

To be able to manage the multitude of mobile devices in the workplace, it is important for an organization to understand what types of devices exist and the features they possess. Many different vendors have their own hardware and software which makes the need for a blanket solution that allows for support of many devices, imperative for an organization. Devices over the years have changed and gained more functionality of what a user can accomplish with the devices as well as increase in the areas that a device can access.

**Smartphones**

Smartphones are probably the most common type of mobile device on the market as they offer a variety of functions such as email, social media interaction, installation of applications and portability. This allows the user to be able to carry a device that can almost function as a personal computer but fit in the user’s pocket. The smartphone is also very easy for the average user to adopt as it is easy for the user to transition from the basic cellphone to the smartphone. Many vendors offer a smartphone, but for the purpose of this paper we need to be able to
understand the different types of operating systems (OS) versions that are available for smartphones. The next section will cover the four major phone operating systems used today.

*Android OS*

The Android OS is developed by Google and by their definition of the Android OS it is a free, open source platform available for anyone to use. The latest version that has been released by Google is Android 4.0 also known as Ice Cream Sandwich (ICS) (Google Inc., 2012). The Android OS runs on all types of phones including HTC, Motorola and others.

*iOS*

The Apple iPhone runs the Apple operating system known as iOS. The current version that is available on the iPhone is iOS 5. This operating is only available for the Apple iPhone and is not open to other smartphone vendors (Apple Inc., 2012).

*Windows Phone OS*

Microsoft has developed an operating system running the Windows Phone 7.5 OS. This operating system allows for a smartphone user to not only do the daily tasks that most smartphones can currently do, but it also is able to sync with an XBOX 360 user account (Microsoft, 2012). The Windows Phone 7.5 OS is available on HTC, Nokia and Samsung devices.

*BlackBerry OS*

Research In Motion (RIM) has developed the OS known as the BlackBerry OS which is currently at version 7.1. The BlackBerry OS was once the mainstream corporate OS and was the top smartphone chosen for the security that the RIM phones provided. The BlackBerry devices require a BlackBerry Enterprise Server (BES) to successfully synchronize corporate email with the mobile device (Research In Motion Limited, 2012).
Netbooks and Laptops

Another form of mobile device that is popular in the workplace is the laptop or the slightly smaller netbook. These devices are popular for traveling staff or users that may frequent onsite locations and need to gain access back into the organization. Laptops or netbooks allow for more versatile applications to be installed outside of the common application stores that other mobile devices offer. While this versatility is convenient, it also allows users to store confidential data directly on the laptop or netbook. A major concern of allowing employees to use these types of devices is being able to secure them not only while in use but also if the device is lost or stolen. It is very easy for someone to gain access to a laptop or netbook if it has not been secured or protected with hard drive encryption software (Zhang, Hu, & Fujise, 2007).

The operating systems that are currently running on laptops and netbooks can be narrowed down to three major systems. Each company has developed many different variations, but for the purpose of this paper the current operating systems will be discussed.

Apple OS

Apple OS X is the current operating system running on the MacBook Air and the MacBook Pro versions of Apple’s laptops. Apple’s laptops have been moving to a more mainstream use based on the fact that their devices are designed slimmer and are esthetically eye catching to users (Apple Inc., 2012).

Microsoft Windows

Microsoft Windows has been around in the corporate world for quite some time and holds most of the market share in this area (Microsoft, 2012). Microsoft has many versions of Windows that will need to be addressed based on which version may currently be running in the
business in question. The major operating systems that are used on laptops and netbooks are the following:

- Windows XP
- Windows Vista
- Windows 7

Linux Distributions

Linux is an open source operating system that has many different versions that have been developed over the years by different groups or organizations. There are three popular distributions of Linux currently used by the growing community (Linux.org, 2012):

- Fedora
- Ubuntu
- Linux Mint

Tablets

Tablets are the newest devices to enter the corporate environment. In fact, tablets are probably the top personal device that employees want to be able to bring into the workplace and utilize within the company. Tablets may not be supplied by the company, but a growing number of employees are either purchasing them for home use or receiving them as gifts from family members. Once they see how versatile they can be at home and on the road, the users want to transition them to the office.

Tablets typically currently come installed with two variations of operating systems that have been previously discussed. Apple has their version of the iPad which runs the iOS, the same operating system as the iPhone (Apple Inc., 2012). There are many other tablet manufacturers that currently offer the Android OS as the choice for their devices (Google Inc., 2012). Another
newcomer is Microsoft with the newly announced Microsoft Surface that will be available in fall of 2012 running Windows 8 (Microsoft, 2012). This device will add another choice for consumers that are looking for traditional functionality they may be used to within the Microsoft family of operating systems.

It is important for an organization to know exactly which devices will be allowed or supported within their environment. For this paper, the author will look at solutions that will allow for support and securing of all mobile devices that are currently available with the latest supported operating systems.

**Mobile Device Benefits**

Mobile devices offer many benefits within the workplace. They allow users to work in the office, out of the office, in conference rooms and at home while maintaining wireless connectivity to access data within the organization. As more and more companies are using the business model of working from home or a remote location for their employees, the idea of mobile devices such as laptops enable this to come to be a possibility.

For many years it was the employer who purchased mobile devices for their employees on a per job role basis. Not everyone was able to qualify for a mobile device based on their job role or job duty. Now more than ever, employees are now introducing the mobile devices into their own homes and are looking for approval to be able to use their own device in the office. Employers can benefit from this as they will not have to purchase or support the hardware for the employee. In the end, the I.T. department will need to make sure that the employee is able to connect into the corporate system. The employee also benefits from purchasing their own device as they can chose which device they would like to use and own and not have the company decide for them the device to purchase.
Although there are many benefits for the corporation and the employee, there are also many security issues that go along with approving users to bring in their own device to the workplace. In the next section, this paper will discuss the security issues or concerns that may arise when introducing personal devices into the workplace.

**Security Concerns**

Security for any organization is always a top priority to make sure that the organization’s data and the clients’ data is secure and protected. Securing devices within an organization is a difficult enough task. Now the I.T. department will need to make sure that all mobile devices, personal and company owned, are secure in all circumstances and situations. The question that this paper will answer is if it is indeed possible to secure all devices in all various circumstances and situations and the best way to achieve that goal of security.

There are many ways or possibilities of how an intruder could gain access to an unsecure device without the proper protection. Tablets and smartphones are just as much at risk as are laptops and netbooks. Tablets and smartphones allow a user to install applications or apps that are published in either the App Store distributed by Apple or Google Play distributed by Google. These apps can contain malware or other malicious software attached within the code (Stallings, 2011).

There are other concerns that will be addressed such as how to deal with the device is it is either hacked or stolen. The next section will discuss how to handle a variety of situations that need to be considered when implementing a strong deployment of personal mobile devices.

**Viruses and Malware**

Most devices such as smartphones or tablets allow for the installation of apps that have been developed specifically for each type of device. Netbooks and laptops allow for the user to
install software at their leisure with a simple download or install. The issue that organizations have to deal with is how to prevent applications that may install malicious software or viruses on the personal devices. It is much easier for an organization’s I.T. department to prevent these types of software from being installed on company owned devices.

*Malware* or Malicious Software is defined as a type of software that is intended to do malicious damage to a computer system (Gollmann, 2006). Preventing this type of software from being introduced into the organization by way of a personal device is a concern.

A *Virus* is defined as a piece of self-replicating code attached to some other piece of code, with a *payload*. A payload could be the popup of random windows on the computer, reducing access to the user’s system or installing software to cause damage to the user’s computer (Gollmann, 2006).

Device Hacking

Any time a user accesses data by way of connecting to some form of wireless network, whether the device is connected to a cellular connection or through a secured or unsecured wireless network, there is a chance that the data accessed can be stolen or the device hacked. *Hacking* is defined as the breaking into computers or networks without the authorization to access those areas (Tipton & Krause, 2007). Many celebrities have had their devices broken into by hackers trying to gather confidential data such as photos or phone numbers. A recent article published in October 2011 describes the criminal activity by Christopher Chaney who hacked into more than 50 celebrity devices including Scarlett Johansson the actress (Shira, 2011). This does not only affect celebrities, but it is also a threat to the individual getting coffee and using the free wireless connection at the local coffee shop.
Lost or Stolen Devices

Another issue to consider when allowing personal mobile device use within the workplace is the possibility of human error. As employees travel for business they are constantly under the pressure of unfamiliar territory and time constraints. Items, such as mobile devices can be misplaced or left unattended where they could possibly wind up stolen. It is important to be able to prevent the data from being stolen or accessed if the mobile device has been lost or stolen. In recent years there have been some high profile stories of devices being lost or stolen. One story that had made headline news back in August 2011 was the report of the Apple employee loosing what was thought to be the iPhone 5 prototype. Basically, the employee was at a Mexican restaurant, Cava 22 in San Francisco and the phone was “misplaced” (Potter, 2011).

Another high profile news headline that made news in January 2011 was that of a UK doctor that had his laptop stolen with patient data loaded on it. The UK doctor had 1,147 patients’ data including names, birth dates and the treatments of the patients loaded on the unencrypted laptop and the device was stolen. The doctor waited two weeks before reporting the stolen laptop (Leyden, 2011).

Any device could be stolen or misplaced. It is very important for any company that is considering using mobile devices, personal or company owned the devices need to be secure and encrypted as accidents do happen.

Compliances for Different Fields

Security policies are designed to protect the data within an organization and to keep trade secrets private. There are many policies that have been designed by organizations or groups that oversee the protection of patients and other individuals from businesses releasing confidential and private data. It is up to each organization to meet these compliances. This section will
discuss which policies are in place and the fact that an organization has to be aware of these policies when considering the use of personal mobile devices.

HealthCare Organizations

Using computers to access confidential patient data within the HealthCare field requires certain rules to follow to protect this confidential data. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was passed to protect the confidentiality, integrity, and availability of electronic protected health information or ePHI (Tipton & Krause, 2007). HealthCare organizations that are considering the use of personal mobile devices must consider the risks involved with this type of implementation and also must be able to be HIPAA compliant.

Financial Institutions

Banks and other financial institutions have a responsibility to manage confidential data when dealing with such important information such as social security numbers, credit card numbers, bank account information, birthdates and other confidential data that are used on a daily basis. A recent security breach that made headlines was the security breach with MasterCard and Visa at a processor branch. This breach was reported in March 2012 and was admitted to be a “massive” breach of possibly more than 10 million card numbers (Krebs on Security, 2012).

Government Agencies

Agencies that are affiliated with the government have to follow many rules and regulations that can easily cover multiple compliances such as HIPAA. The government offices have to deal with many forms of confidential data including social security numbers, driver’s license numbers and tax information just to name a few (Layton, 2007).
Private Corporations

Private businesses or organizations generally have specific policies and procedures in place that are specific to the organization. However, if the organization conducts business with any specific group such as insurance agencies, healthcare organizations, or government agencies, the private company must be compliant according to the laws in those fields also.

It is very important when deciding to implement personal mobile devices to make sure that all rules and regulations are followed based on the type of business that is conducted within an organization and the partners that the company conducts business with.

Survey

Before the methods of this paper are discussed the author will conduct a survey that will allow for study of how other companies are currently handling the use of personal mobile devices within the workplace. It is expected that some of the individuals that participate in the survey will respond that their company does not allow the use of the personal devices where they are employed. The survey will be conducted through the Survey Monkey web portal (SurveyMonkey, 2012). Through this survey, the author will determine some outcomes after analyzing the data. The survey will be discussed in greater detail in the methodology section of this paper and can be viewed in the Appendices section as Appendix A.

Software Evaluation

This paper will present three possible software solutions that will be investigated to determine which software implementation may offer the best solution for an organization. The software solution should meet all of the needs and be able to support the devices and operating systems that the organization has implemented. It would not be beneficial to implement software that is able to handle most of the devices, but not be able to handle tablets for example. It is also
not ideal for I.T. departments to have to support multiple software tools to manage mobile devices.

The three different software tools that this paper will discuss are MaaS360, Zenprise and the tools that are offered by Microsoft Exchange Server 2010. Each one of these solutions offers a variety of features that allow an organization to handle mobile devices.

MaaS360

Fiberlink Communications cooperate headquarters is located in Pennsylvania, United States and produces a product called MaaS360. MaaS360 offers a variety of features that cover devices ranging from mobile devices and also laptops (Fiberlink Communications Corp., 2012).

MaaS360 is a solution that is well-rounded and offers many features for an organization to be able to implement and manage the mobile devices and laptops that may be used within the workplace. Fiberlink describes the MaaS360 platform as “One Window. One System. All Your Devices.” (Fiberlink Communications Corp., 2012). MaaS360 is a very flexible solution that offers an I.T. department the following characteristics as described by the organization’s website:

- Integration
- Manageability
- Security and Compliance
- Scalability
- Multi-tenancy
- Vendor Viability

MaaS360 gives the control to the organization’s I.T. department that allows many solutions to the issues that have been discussed previously such as how to handle a lost or stolen
device, preventing certain applications from being installed and making sure that the device is secure and to be compliant when being used in the workplace.

MaaS360 covers all the major mobile devices such as the iphone, ipad, Android, Windows Phone, BlackBerry and the Kindle Fire (Fiberlink Communications Corp., 2012). Having the control of all of the different brands is important to a universal support option.

MaaS360 offers two pieces of the puzzle when it comes to managing devices. The first part is the Mobile Device Management (MDM) portion which allows for the management of mobile devices including PDAs, Smartphones, and Tablets. The other portion of MaaS360 is Laptop Management which allows for the support and management of laptops.

Mobile Device Management (MDM)

MaaS360 Mobile Device Management offers many features to help manage these mobile devices as shown in the following list (Fiberlink Communications Corp., 2012). A more detailed description of these features can be found in the Appendices section as Appendix B.

- Device Quarantine and Approval
- Enterprise Application Catalog
- Integration with Existing IT Infrastructure
- Bring Your Own Device (BYOD)
- OTA Configuration Management
- Remote Wipe
- User/Device Enrollment and Device Discovery
- Detailed Visibility into all Devices
- Help Desk Operations
- Policy Management and Enforcement
• Mobility Intelligence Dashboards
• Passcode and Device Restriction Policies
• Restrict Applications

Managing the organization’s laptops needs to be addressed as well. With the MaaS360 Laptop Management, located within the same platform, it is possible to do this from one platform. While laptops are out on the road or out of the office the data that is accessed and saved on the laptop needs to also be secured. The Laptop Management offered by MaaS360 has many features to allow for management of these devices. MaaS360 Laptop Management features that are available are shown in the following list (Fiberlink Communications Corp., 2012) and can be found in more detail in the Appendices section as Appendix C.

• Application Updates
• Hardware Inventory
• Persistent Policy Management
• Software Distribution
• Endpoint Security
• Patch Management
• Remote Device Control
• Software Inventory

While reviewing the MaaS360 software by Fiberlink, it was noted that the software offers many features and options from the console that covers all of the major mobile devices on the market from one platform. This is a great feature when an organization is deciding on mobile device management software.
Zenprise

Zenprise is a company located in California which offers a mobile device management software solution. The solution, Zenprise MobileManager, offers support to manage devices such as the iPhone, iPad, Android, BlackBerry, Symbian and Windows Mobile (Zenprise, 2012).

Zenprise states on the website that MobileManager allows an organization to be able to manage the mobile devices by being able to do the following (Zenprise, 2012):

- Configure
- Provision
- Secure
- Support
- Monitor
- Decommission

Having this control within an organization can allow for personal mobile devices to be managed and secured according to the policies that are in place. Zenprise is a valid solution for mobile devices, but the company does not offer a solution for laptops. If an organization were to choose Zenprise for mobile management, another laptop management solution would then have to be implemented.

Microsoft Exchange 2010

If an organization is using Outlook as the email client and are running Microsoft Exchange 2010 for the server, there are some features that are built into Exchange 2010 that allows management of mobile devices.

Microsoft Exchange Server 2010 allows an I.T. department to be able to wipe, block and reset a mobile device remotely and manage the devices with policy management. (Microsoft
Corporation, 2011). Unfortunately, the management is limited to mostly email and not the applications that a user can or cannot install unlike the previous software discussed. Files that may have been downloaded or saved on the mobile device could still be available to access by a hacker or an unauthorized individual. This solution is well suited for organizations that are not able to purchase a third party solution but want to be able to have some control over mobile devices.

**Methodology**

The methods that will be used to collect the data will include the following to be able to gain knowledge and an understanding if it is possible to employ personal devices in the workplace.

**Conduct Survey**

The survey will help the author understand how other fields are considering, handling or implementing the concept of personal mobile devices within the workplace. The survey was taken by 100 people who are currently employed in multiple fields of industry. This will allow the author to get a feel of how multiple types of organizations are currently handling personal mobile devices and also if users are knowledgeable with their companies policies.

The survey can be viewed in its entirety in the Appendices section as Appendix A.

**Develop Policies and Procedures**

Policies and Procedures will need to be developed to help the end-users understand what can and cannot be accessed or installed while using a personal device on the organization’s network. These guidelines will help not only to inform the employees of what can and cannot be performed while accessing the companies data, but the policies will also help the I.T. staff to have a clear understanding of the rules to present to the end-users for reference. A sample
process of developing policies can be found in the Appendices section as Appendix D (Ruskwig, 2011). Intel’s Social Media Guidelines can be found in the Appendices as Appendix E (Intel Corporation, 2012).

### Develop Authorization Request Form

The authorization form will need to be created to make sure that all parties understand the policies and procedures and acknowledge them by signing the request form.

### Trial the Software

Finally, the software that is available for the organization and the I.T. department must be trialed to make sure that all areas of interests are covered and that the software meets all of the requirements by the organization. The author will evaluate and investigate the three software solutions that were mentioned previously to make a decision based on features and coverage for what might be accepted by most organizations.

### Results

To be able to put together a plan to allow for a successful implementation, it is very important to understand the security risks that have to be prevented, the policies that needed to be created and the types of devices that a corporation may have to deal with to allow for personal mobile devices to be incorporated into the organization’s environment.

This next section will help an organization to be able to design the process that will aid organizations’ to allow for personal mobile devices deployed in a secure fashion. Policies and procedures need to be created to make sure that the employees understand what has been approved and not approved to do on the personal device that is being used in the workplace.
Policies and Procedures

It is important for an organization to have formal guidelines for employees to be able to understand what is expected of them and how they must conduct themselves while using their personal mobile device in the workplace. The first step to implementing the use of personal devices is to make sure that proper policies and procedures are in place to help the employee understand what is required of them and the guidelines that they need to follow. To help draw up the policies and procedures it is important to be able to understand how to begin this process. To do this a few questions must be answered by the organization looking to implement the use of personal devices.

- Which devices are acceptable to be used on the company’s network?
- Does the company need to control which apps are installed?
- Does the user understand that the company will have certain access and requirement restraints as long as the device is accessing the company’s data?
- Does the company want to enact a remote wipe tool to prevent data leakage if the device is lost or stolen?

These questions will need to be included within the policies and procedures documents for users to read and then acknowledge in writing for accountability that they do understand the policies that enable them to use their personal device to access company data. A sample policies and procedures can be viewed in the Appendices section as Appendix F (Business Link, 2012).

Approval Request

Once the policies and procedures have been created and published, it is important to have a document created that the employee can sign to acknowledge that he or she understands and will be accountable for what is expected of them. This document, or the Personal Mobile Device
Request form, should be signed not only by the employee requesting access and by the employee’s superior but also the Security Administrator within I.T. A sample of this document can be located in the Appendices section as Appendix G.

Once the approval request has been completed, then it will be up to the I.T. department to setup and configure the user’s device to work with the company data and email. To be able to achieve this, it is important to have software in place to be able to manage the devices.

**Software Selection**

For this paper, MaaS360 has been selected as the appropriate application software to meet the needs of all mobile devices including laptops. With this software, the I.T. department can manage the devices and configure them to be used properly while accessing the company data.

Now that the software has been selected, the configuration needs to be completed and the security policies put into place to make sure that the personal mobile devices meet the requirements that are needed for them to operate safely.

**Applications**

Applications from app stores, whether through Apple or Google, can be infected with a virus or malware. To prevent the infection of a mobile device that is accessing company data, I.T. can restrict the installation of applications that are not approved for installation. More so, I.T. can push out the installation of the supported applications by using MaaS360 which allows the proper installation of secure and clean applications. If applications are installed that are not approved, the device user will be warned that an unauthorized application has been installed and must be removed within 24 hours to continue to use the device with the corporate data and access.
Device Security

Next, it is important to make sure that the devices that are accessing company data have the proper access security setup on the device. This means that the device will require a pin code or some other form of security access code to be able to use the data or the device itself. This setting will be a standard policy that is configured for the mobile devices that are accessing company data.

Rooted Devices

Device rooting is defined as removing the restrictions on a device to allow access to low-level functions (The Computer Language Company Inc., 2012). If a device is rooted, it will not be allowed to access company data. A rooted device may allow for more user control of the device but a rooted device can also allow unwanted software intrusions or a less secure device.

Survey Results

The survey that was gathered from the 100 individuals who took the survey was very useful in understanding the trend with organizations using mobile devices and more specifically personal mobile devices within the workplace.

The major types of industry that were selected by the surveyors including the percentage of the specific field are shown below. The author’s intention was to be able to include the major types of field that are overlooked by organizations or groups making sure compliances or policies are followed. If the organization did not fit into the specific fields that the author was looking for, those results were then included in the Private Organization group.
The majority of the fields that were given for answers in the survey fell into the Private organization. HealthCare Institutions was the second top selection in the survey.

- 52% Private Organization
- 28% HealthCare Institution
- 8% Financial Institution
- 6% Education
- 6% Government Organization

The Fields of Employment chart can be viewed in the Appendices as Appendix H.

Of the 100 people that were interviewed, there were a total of 152 mobile devices being used by those individuals. Some of the surveyors that were interviewed are using multiple devices such as a smartphone and a laptop or even more devices than just two.

Of the 152 devices that were reported being used, only 81 of those devices were reported as being used for work purposes. The number 81 will be the number that will be referenced in the following charts as the base number since the survey results that we are looking for are mainly with the devices that are used within an organization’s network and accessing company data.

Another data figure to be aware of is that out of the 81 devices used for work purposes 40 of them were personally owned. This means that almost half of the devices surveyed were company owned and almost half of the devices were personally owned. These numbers can be viewed in the Appendices as Appendix I.

Security is always a large concern for any organization. Any form of security breach or data loss could be very detrimental for an organization. One of the major forms of data access for a mobile device is corporate email. Most individuals that use mobile devices use them out of the
office which means they are consistently checking their email to keep in contact with the main office.

Of the 81 devices that are used for work purposes, there are 40 laptops that receive company email on the device, 27 smartphones that receive company email, 10 tablets that receive company email and 4 netbooks that receive company email. As the data shows, all 81 of the devices receive company email on the mobile devices. This is an interesting result as it will be up to the organization to be able to prevent the email from being accessed by the wrong individual if the device was to be stolen or lost. The data can be viewed in the Appendices as Appendix J.

Now that the survey results have shown that there are employees using personal and company owned devices to access company email and other resources on the company network, are any of these devices password or pin number protected?

It was reassuring to see that 64 of the 81 devices did have some form of security in place that requires a user to either enter a password or a pin number to access the device. However, the number that is very concerning is the remaining 17 of the 81 devices that do not have any form of protection in place. This could be a major security concern if the device were to be lost or stolen. It is very important for any organization to understand that it is better to implement security precautions than try to explain to the clients or business partners how a security breach took place on an unsecured device. The breakdown of this data can be viewed in the Appendices as Appendix K.

Lost devices or stolen devices are always a concern as users travel from place to place conducting work while on the road. One question that was asked in the survey was if the surveyor had ever lost or had a device stolen. Out of the 100 users that used 152 mobile devices,
there was only 1 device reported lost or stolen. Based on the survey results, the device that was
lost was a company owned laptop that had security protocols in place. The results from the
survey can be viewed in the Appendices as Appendix L.

The following sections will discuss the results of the survey that deal with the policies
and procedures that the organizations may have in place, if the organizations allow personal
mobile devices in the workplace and if any of the employees had to sign formal documentation
to be able to access the company network and data.

Policies and procedures are the foundation of any good security plan. It is important for
employees and the organization to understand how to handle and use mobile devices and
personal mobile devices within the infrastructure.

Of the 100 individuals surveyed, 62 of them stated that their employers do allow the use
of personal mobile devices for work purposes within the organization that they currently work.
However, 38 of them said that their place of employment does not allow the use of the personal
devices. These results can be viewed in the Appendices as Appendix M.

Other information that the author was looking to gather from the survey was how the
employers handled the implementation of the personal mobile devices. The organizations should
have policies and procedures in place to handle mobile devices. This part of the data could be
accurate, however it may not be reliable as some employees may not know if specific policies
and procedures do exist. The data collected shows that 72 people out of the 100 surveyed stated
their employer does have specific policies and procedures in place to inform their staff. On the
other hand, 28 out of 100 surveyors stated that their employer does not have anything in place to
inform the employees of personal mobile device use. This data could reveal that the organization
does not have any published policies on personal mobile device use or that the employees just aren’t aware of them. Appendix N shows the data collected from the survey.

The last portion of the data that was collected reports if the user’s employer requires a formal document to be signed to access company data with a personal mobile device. The data collected from the survey shows that 65 of the 100 people surveyed stated that their employer does not require a document to be signed and 35 people stated that their employer does require a formal document to be signed. Appendix O shows the results.

The survey allowed the author to be able to collect data to gain an understanding of how organizations in other fields are currently implementing the use of personal devices. Through the data collected, it appears that more organizations are allowing the use of these devices.

**Recommendations**

The author would recommend for any organization that is contemplating the idea of implementing personal mobile devices to make sure to have a strong foundation of policies and procedures before deploying the devices. The policy and procedures allow for all parties, the organization and the employee, to understand what is expected of them and how to proceed with using the mobile devices. The policies protect the employee as well as the organization.

It is also important to understand that the author selected the software MaaS360 as the software of choice for this paper. However, the organization will need to consider the features that are important to meet the needs of the organization, the budget that is available to the organization and also keeping in mind the devices that will need to be supported before choosing an appropriate software application.
Mobile devices have been gaining an increase in the market share and have been making a larger impact in the corporate world with more users utilizing mobile devices to conduct daily business. Smartphones, tablets, netbooks and laptops are the types of devices that are used on a regular basis not only in the workplace but also in individuals’ homes. The trend that seems to be growing is that an increased number of employees are asking for approval to bring and use their personal devices within the workplace.

Is it possible to embrace personal mobile devices within a company and maintain the security needed for the company and client’s data? Yes, this is possible for an organization to implement as long as security and data protection is top priority. Policies and Procedures along with the correct software implementation can allow for personal devices to exist within the workplace allowing for flexibility and ease of implementation.

Bring Your Own Device or B.Y.O.D. is an idea that is gaining ground and more companies are opening up to the idea to enjoy the benefits and flexibility that the use of personal mobile devices in the workplace has to offer for the organization and the employees.
References


http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1076142205&type=RESOURCES

http://www.maas360.com/


http://www.theregister.co.uk/2011/01/19/hull_hospital_data_breach_flap/

http://www.linux.org/article/view/selected-a-linux-distribution


http://us.blackberry.com/


http://www.ruskwig.com/it_security_policy.htm


http://www.people.com/people/article/0,,20536767,00.html


http://www.surveymonkey.com/home/

http://www.pcmag.com/encyclopedia_term/0,1237,t=rooted+device&i=63340,00.asp


Appendices

Appendix A Survey

Bring Your Own Device to Work

You are cordially invited to participate in a research study. The purpose of this research study is to determine the use of personal mobile devices in the workplace. If you participate in this research, you will be asked to take a 5 minute anonymous web survey.

You must be 18 years or older to participate in this survey.

Your participation will take approximately 5 minutes to complete.

Your participation in this research is strictly voluntary and anonymous. You may refuse to participate at all, or choose to stop your participation at any point in the research, without fear of penalty or negative consequences of any kind.

The information/data you provide for this research will be treated confidentially, and all raw data will be kept in a secured file by the principal investigator. Results of the research will be reported as aggregate summary data only, and no individually identifiable information will be presented.

You also have the right to review the results of the research if you wish to do so. A copy of the results may be obtained by contacting the principal investigator at the email address below:

Jim Hess
jmhess22@hotmail.com

There will be no direct or immediate personal benefits from your participation in this research.

I understand that this research study has been reviewed and Certified by the Institutional Review Board at Davenport University. For research-related problems or questions regarding participants’ rights, I can contact Davenport’s Institutional Review Board at IRB@davenport.edu.

I have read and understand the information explaining the purpose of this research and my rights and responsibilities as a participant. By selecting the choice to agree below designates my consent to participate in this research study, according to the terms and conditions outlined above.

☐ I agree that I am 18 years or older and would like to take this survey

☐ I do not agree to take this survey

☐ I am not 18 years or older
### Bring Your Own Device to Work

<table>
<thead>
<tr>
<th><em>Which type of industry are you employed?</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Financial Institution</td>
</tr>
<tr>
<td>☐ Government Organization</td>
</tr>
<tr>
<td>☐ HealthCare</td>
</tr>
<tr>
<td>☐ Private Company</td>
</tr>
<tr>
<td>☐ Currently Unemployed</td>
</tr>
<tr>
<td>Other (please specify)</td>
</tr>
</tbody>
</table>


Which of the following devices do you currently use?

- Laptop
- Netbook
- Smartphone
- Tablet
- None
**Which of the following devices do you currently use for work purposes?**

- Laptop
- Netbook
- Smartphone
- Tablet
- None
### Bring Your Own Device to Work

*Which of the following devices that you use for work purposes are personally owned?*

- Laptop
- Notebook
- Smartphone
- Tablet
- None
### Bring Your Own Device to Work

*Do you receive company email on any of your devices?*

- [ ] Laptop
- [ ] Netbook
- [ ] Smartphone
- [ ] Tablet
- [ ] No
Bring Your Own Device to Work

* Do any of your devices have some form of password protection or require a pin number to gain access to the device?

- Laptop
- Netbook
- Smartphone
- Tablet
- No
Bring Your Own Device to Work

*Have you ever lost or had any of the following devices stolen?

- Laptop
- Netbook
- Smartphone
- Tablet
- No
Bring Your Own Device to Work

* Does your employer allow employees to use personal devices for work purposes?

- Yes
- No
Bring Your Own Device to Work

* Does your employer have specific policy and procedures regarding the usage of personal devices in the workplace?

☐ Yes
☐ No
### Bring Your Own Device to Work

* Does your employer require employees to sign any documentation to allow the use of personal devices for company email or data?

- [ ] Yes
- [ ] No
Bring Your Own Device to Work

Thank you for taking this survey!
Appendix B MaaS360 Mobile Device Management (MDM)

Quickly deploy and support mobile devices in the Enterprise
IT organizations today need visibility into and control over the mobile devices that are entering the enterprise, whether they are employee-owned or provided by the corporation. MaaS360 mobile device management provides a comprehensive, complete set of capabilities to get devices configured for enterprise access and to make sure corporate data stored on these devices is secure.

Device Quarantine and Approval
Notifies IT of any new devices on the network and enables blocking or approving them, thus ensuring compliance with corporate policies.

Enterprise Application Catalog
Provides a private, enterprise-wide system to advertise, distribute and update in-house developed and enterprise specific applications recommended by the enterprise, plus access to public application catalogs.

Integration with Existing IT Infrastructure
Integrates seamlessly with Exchange ActiveSync, Lotus Notes Traveler and Outlook to make device support more secure and compliant. Leverage the features of Active Directory to authenticate enrollment requests and place users into logical groupings.

Bring Your Own Device (BYOD)
Allows your users to connect with their own devices and enforce your corporate policies. You can choose to approve or block devices, provide a self-service support portal, and selectively wipe them if necessary.

OTA Configuration Management
Delivers and maintains corporate device profiles, including Wi-Fi and VPN settings.

Remote Wipe
Monitors the data leak risk of lost or stolen devices. Complete remote wipe removes the device to factory defaults; selective wipe can remove corporate data while preserving personal data intact.

User/Device Enrollment and Device Discovery
Provides efficiencies by allowing users to enroll their own devices, and with automated device discovery reports and notifications.

Detailed Visibility into All Devices
Provides information about software and hardware inventory, including model, serial number, OS, roaming status, and configuration and vulnerability details.

Help Desk Operations
Lets your IT staff perform typical Help Desk tasks like sending a message, locating a lost device, isolating a device, or resetting a forgotten password.

Policy Management and Enforcement
Controls manage and distributes policies to your devices. Enforces policies for passwords and encryption to ensure your users have minimum level of protections. Also identifies stolen or rooted devices.

Mobility Intelligence™ Dashboards
Analytical and reporting related to mobile device operations and compliance. Gain insight into the distribution of mobile devices across mobile operating system platforms, approvals, device capabilities, ownership and various other details.

Passcode and Device Restriction Policies
Controls approved devices to protect the device from theft, and restrict unapproved features and applications.

Restrict Applications
Selectively monitors and restricts specific applications and features on each device, allowing you to prevent data roaming, Bluetooth and tethering.
Appendix C MaaS360 Laptop Management

Laptops - the original mobile device in your Enterprise Device Management strategy

Whether you’re optimizing your existing laptop management strategy or considering total enterprise device management to include smartphones and tablets, the challenges are the same: dealing with constantly changing users, devices and applications, preventing security risks and illegal information access, and aligning user expectations and asset management.

Application Updates
Provides the visibility and centralized command and control to eliminate multiple versions of applications, and ensure the latest application updates are installed.

Hardware inventory
Manages and supports your devices in all operations throughout their lifecycles. Inventory reports provide identification information, data necessary for hardware refreshes, and critical information needed for planning software rollouts.

Persistent Policy Enforcement
Allows you to customize a policy to monitor specific types of software, and then require an action when a device falls out of compliance. For example, you can disconnect a device from the corporate VPN if anti-virus definitions are out of date.

Software Distribution
Allows you to create packages containing documents and applications and deploy those packages to your users. This allows you to make sure your users have what they need to be productive while their data stays safe.

Endpoint Security
Monitors and reports on all your critical security applications, regardless of vendors, to ensure compliance with corporate policies from start up to shut down, even while off the corporate network.

Patch Management
Ensure your devices have the latest security patches and updates, regardless of whether they are on your corporate LAN or just connected to the Internet. View critical information about available patches, including the size, severity level and how many of your users are missing each one.

Remote Device Control
Integrates seamlessly with a customer’s existing remote control or desktop applications to allow IT to launch and initiate connections to remote devices directly from MaaS360 without the need for additional tools for real-time information gathering, user interaction, or manually launching the remote control application.

Software Inventory
Track and audit installed applications day-to-day, checking for dangerous installed software, supporting end users, and identifying ways to save money on expensive applications that are not being used.
Appendix D Process of Developing Security Policies

SECURITY POLICY - IT SECURITY POLICY

The essence of an IT security policy is to establish guidelines and standards for accessing the organisation's information and application systems. As IT infrastructures have become more complex and organisations' resources have become more distributed, the need for improved information security has increased.

An IT security policy facilitates the communication of security procedures to users and makes them more aware of potential security threats and associated business risks. A written IT security policy helps to enhance the performance of the organisation's IT security systems and the e-business systems that they support.

Surveys regarding IT security all tend to show similar trends:
- Most organisations have been the victims of security breaches.
- IT security breaches cause significant damage.
- IT security breaches are increasing.
- Insiders pose a significant threat as outsiders.

If an organisation suffers an IT security breach it is likely to suffer negative impact. There are many costs associated with a security breach:
- Direct financial loss.
- Loss of sales and reduced competitive advantage.
- Damage to organisation reputation and brand.
- Business disruption.

An IT security policy mitigates the organisation's legal exposure. The security policy guides the behaviour of employees. Having a written IT security policy is essential if the organisation wants to be able to hold employees accountable for their actions.

An IT security policy forces an organisation to make safer investment decisions. Whilst developing an IT security policy the organisation will have to make intelligent business decisions about the cost effectiveness of reducing or eliminating business risks.

Developing and IT Security Policy

To develop an IT security policy a task force needs to be established and the task force will need to work through the following steps:

1. Access the requirements.
2. Identify the information assets, systems, and facilities.
3. Identify the threats to the assets.
4. Assess the risks to the assets.
5. Develop an IT security policy to mitigate the risks.
6. Implement the security policy.
7. Communicate the policy.
8. Enforce the policy.
9. Re-assess the security policy.

IT Security Policy Contents

The IT security policy should deal with security threats to the organisation's information assets with respect to the following fundamental areas:

- Authentication - ensuring a user is who he says he is.
- Authorisation - controlling what information and applications a user can access.
- Privacy and data integrity - preventing unauthorised users from seeing certain information, and preventing them from making unauthorised changes or deletions.
- Non-repudiation - making sure that parties in a transaction cannot deny what they said or what they did.
- Disaster recovery and contingency planning.
- Physical security.

In some countries today simple passwords only use identification schemes are considered to be inadequate. Two-factor authentication consisting of something you know (a password or pin) plus something you possess (something with digital certificates) is now considered to be the norm.

The IT security policy should have sections dealing with the following issues:

- Access control
- Electronic mail
- Internet security
- Laptops, notebooks and handhelds
- Software security
- Network security
- Physical security
- Auditing and monitoring
- Contingency planning

Implementing the IT Security Policy

Once the IT security policy has been written it needs to be put in place within the organisation. It needs to be communicated to employees, contractors and other personnel to ensure that they understand the security policy and what is required.

The IT security policy will then need to be enforced. IT and security staff will need to implement its contents. They will need to manage user accounts, passwords, group membership, two-factor authentication devices such as smartcards and digital certificates.

The rapid pace of technological change and use of the Internet mean that new security threats appear all the time. The IT security policy will therefore need updating on a periodic basis.

IT Security Policy Summary

An IT security policy is a formal statement of the rules that employees and others must follow when using an organisation's IT infrastructure. Its purpose is to set down procedures for protecting the organisation's information assets.
# Appendix E Intel Social Media Guidelines

## Intel Social Media Guidelines

Social media is changing the way we work, offering a new model to engage with customers, colleagues, and the world at large. We believe this kind of interaction can help you to build stronger, more successful business relationships. It’s a way for you to take part in global conversations related to the work we are doing at Intel and the things we care about.

These are the official guidelines for participating in social media for Intel. If you’re an Intel employee or contractor creating or contributing to blogs, wikis, social networks, virtual worlds, or any other kind of social media, these guidelines are for you. They will evolve as new social networking tools emerge, so check back regularly to make sure you’re up to date.

Participation in social computing on behalf of Intel is not a right but an opportunity, so please treat it seriously and with respect. If you want to participate on behalf of Intel, take the Social Media Pit Stop training and contact the Social Media Center of Excellence. Please read and follow the Intel Code of Conduct. Failure to abide by these guidelines and the Intel Code of Conduct could put your participation at risk. Contact socialmediagenre.com for more information. Please also follow the terms and conditions for any third-party sites.

### 1. Disclose
Your honesty—or dishonesty—will be quickly noticed in the social media environment. Please represent Intel ethically and with integrity.

- **Be transparent:** Use your real name, identity, that you work for Intel, and be clear about your role.
- **Be truthful:** If you have a vested interest in something you are discussing, be the first to point it out and be specific about what it is.
- **Be yourself:** Stick to your area of expertise, write what you know. If you publish to a website outside Intel, please use a disclaimer something like this: "The postings on this site are my own and don’t necessarily represent Intel’s positions, strategies, or opinions."

### 2. Protect
Make sure that all transparency doesn’t violate Intel’s confidentiality or legal guidelines for commercial speech—or your own privacy. Remember, if you’re online, you’re on the record—everything on the Internet is public and searchable. And what you write is ultimately your responsibility.

- **Don’t tell secrets:** Never reveal Intel’s classified or confidential information. If you’re unsure, check with Intel PR or the Global Communications Group. Off-limits topics include: litigation, non-public financials, and unannounced products. Also, please respect brand, trademark, copyright, confidentiality, and trade secrets. If you give it, you lose it; please rather publish.
- **Don’t use the company (or Intel) Trademarks:** Flip-flops. Anything you publish must be true and not misleading, and all claims must be substantiated and approved. Product benchmarks must be approved for external posting by the appropriate product benchmarking team.
- **Don’t overshare:** Be careful out there—one day you’ll regret it. Post being judicious will help keep your content more crisp and audience-relevant.

### 3. Use Common Sense
Perception is reality, and in online social networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as an Intel employee, you are creating perceptions about your expertise and about Intel. Do as we all know.

- **Add value:** There are millions of words out there—make yours helpful and thoughtful or insulting. Remember, it’s a conversation, so keep it real. Build community by posting content that invites responses—and stay engaged. You can also broaden the dialogue by citing others who are writing about the same topic and allowing your content to be shared.
- **Keep it civil:** There can be a fine line between healthy debate and inflammatory rhetoric. Try to frame what you write to invite differing points of view without influencing others. You don’t need to respond to every criticism or data. Be careful and considerate.
- **Did you trip up?** If you make a mistake, admit it. Be upfront and be quick with your corrections. If you’re posting to a blog, you may choose to modify an earlier post—just make it clear that you have done so.

## Contractors and Endorsements
As the Intel Social Media Guidelines, we support transparency and are committed to clear disclosure of relationships and endorsements. If you are contracted, seeded, or in any way compensated by Intel to create social media, please be sure to read and follow the Intel Sponsored, Seeded, or Incentivized Social Media Practitioner Guidelines. As part of these guidelines, you need to disclose that you have been seeded or otherwise compensated by Intel. Your blog will be monitored for compliance with our guidelines and accurate descriptions of products and claims.

### Moderation
Moderation (reviewing and approving content) applies to any social media context we participate on behalf of Intel. It can be on- or off-site. We do not endorse or take responsibility for content posted by third parties, n.a. user-generated content (UGC). This includes text, audio, visual, and documents. While we strongly encourage user participation, there are some guidelines we ask third parties to follow to keep the site safe for everyone.

- **Post moderation:** Even when a site requires the user to register before posting, simply user name and email address does not validate the person. To ensure lowest risk, we require moderation of all UGC posts. The designated moderator scans all posts to ensure they adhere to Intel’s guidelines.

### Community moderation (a.k.a. reaction moderation)
For established, healthy communities, group moderation by regular users can work well. This will sometimes be allowed to take the place of post-moderation—but it must be applied for and approved.

- **The “house rules”** Where content is post-moderated or community moderated, we use this rule of thumb: the good, the bad, but not the ugly. If the content is positive or negative and not in context, then it can be approved, regardless of whether it’s favorable or unfavorable to Intel. But if the content is ugly, offensive, derogatory, and/or completely out of context, then we ask our moderators and communities to reject the content.

## Intel Sponsored, Seeded, or Incentivized Social Media Practitioner Guidelines
Intel supports transparency. We are committed to ensuring that our social media practitioners (SMPs) clearly disclose relationships and endorsements, and that statements about Intel products are truthful and substantiated. If you are a social media practitioner who has been seeded with products, incentivized, or otherwise has an ongoing relationship with Intel, these guidelines apply to you. If you have any questions or concerns about them, get in touch with your Intel sponsor.

Please keep in mind that Intel mentors social media relative to our business, including the activities of our sponsored, seeded, or incentivized SMPs. If we find any non-disclosed relationships or undisclosed statements that are false or misleading, we will contact you for correction. If, as a sponsored SMP, you are found to be misrepresenting Intel statements about Intel, Intel products, or Intel services, we may discontinue our relationship with you.

### Rules of Engagement for Intel Sponsored, Seeded, or Incentivized SMPs

- **Be transparent:** Please clearly and conclusively disclose your relationship to Intel, including any incentives or sponsorships. Be sure this information is readily apparent to the public and to readers of each of your posts.
- **Be specific:** Do not make general claims about Intel products, but talk specifically about what you experienced.
- **Be yourself:** We encourage you to write in the first person and stick to your area of expertise as it relates to Intel technology.
- **Be conscientious:** Keep in mind that what you write is your responsibility and failure to abide by these guidelines could put your Intel sponsorship or incentive at risk. Also please always follow the terms and conditions for any third-party sites in which you participate.
Acceptable internet use policy - sample template

Use of the internet by employees of [business name] is permitted and encouraged where such use supports the goals and objectives of the business.

However, [business name] has a policy for the use of the internet whereby employees must ensure that they:

- comply with current legislation
- use the internet in an acceptable way
- do not create unnecessary business risk to the company by their misuse of the internet

Unacceptable behaviour

In particular the following is deemed unacceptable use or behaviour by employees:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about [business name], your colleagues and/or our customers on social networking sites, ‘blogs’ (online journals), ‘wikis’ and any online publishing format
- revealing confidential information about [business name] in a personal online posting, upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of malicious software into the corporate network

Company-owned information held on third-party websites

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of [business name]. This includes such information stored on third-party websites such as webmail service providers and social networking sites, such as Facebook and LinkedIn.

Monitoring

[business name] accepts that the use of the internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business.
In addition, all of the company's internet-related resources are provided for business purposes. Therefore, the company maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Sanctions

Where it is believed that an employee has failed to comply with this policy, they will face the company's disciplinary procedure. If the employee is found to have breached the policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal. The actual penalty applied will depend on factors such as the seriousness of the breach and the employee's disciplinary record. [These procedures will be specific to your business. They should reflect your normal operational and disciplinary processes. You should establish them from the outset and include them in your acceptable use policy.]

Agreement

All company employees, contractors or temporary staff who have been granted the right to use the company's internet access are required to sign this agreement confirming their understanding and acceptance of this policy.
Appendix G Personal Mobile Device Use Request Sample

Sample Organization

Procedure: Request for Connectivity of Personal Computerized Equipment to the Sample Organization Network or a Component of the Infrastructure

Objective

The following procedure describes the process of requesting the approval to connect associate personal computerized equipment to the Sample Organization infrastructure as well as the documentation requirements for the connection specifics.

Process

1. The individual requesting the connectivity must provide the attached form completely filled out to SampleIT@sampleorganization.com in advance of the date needed unless an emergency or crisis is in progress.

2. By signing the form below, the individual requesting connectivity agrees to comply with the following:
   - Sample Organization Internet Electronic and Voicemail Policy
   - Sample Organization Data Security Policy
   - In the event that your personal equipment is lost, Sample Organization reserves the right to setup the equipment to ensure that we can remotely scratch the data on the device, making either the data or possibly the device useless.

Records

- File or form name: Request For Personal Connectivity
- File or form location: Policies and Procedures Manual
- Minimum retention duration: 12 months

Revision Records

Initial Document v. 1.0 6/25/12 – Sample Writer
## Sample Organization

**IT Infrastructure**

<table>
<thead>
<tr>
<th>Requestor’s name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requestor’s address:</td>
<td>Phone:</td>
</tr>
<tr>
<td>Requestor’s email address:</td>
<td></td>
</tr>
<tr>
<td>Connection type:</td>
<td>□ PDA/Phone   □ Tablet   □ Netbook   □ Laptop</td>
</tr>
</tbody>
</table>

**Business Case for connectivity:**

Devices needing Access to:

**Name of requestor:**

**Signature of requestor:**

**Name of VCRC Approver**

**Signature of VCRC Approver:**

---

Request approved:

**IT Infrastructure Manager**

**Date**

---

**Document ID:** Revision 1
**Title:** PA Request
**Level:** 0
**Page:** 2 of 3
**Date:** 06-25-12
Sample Organization

IT Infrastructure

NOTES: All Networked Access to be monitored and logged.

Setup performed by: ________________________________
Connection Specifics: ________________________________

__________________________________

Special Notes:

__________________________________

__________________________________

__________________________________
Appendix H Fields of Employment

Fields of Employment

- Education: 52%
- Financial Institution: 8%
- Government Organization: 6%
- Healthcare Institution: 28%
- Private Organization: 6%
Appendix I Mobile Device Use Summary

- Individuals Using Mobile Devices = 152
- Individuals Using the Same Mobile Devices for Work Purposes = 81
- Mobile Devices Used for Work that are Personally Owned = 40
Appendix J Receives Company Email on the Device

Receives Company Email on the Device

- Laptop: 40
- Netbook: 10
- Smartphone: 27
- Tablet: 4

Legend:
- Laptop
- Netbook
- Smartphone
- Tablet
Appendix K Users that Utilize a Pin Number or Password

Users that Utilize a Pin Number or Password

- Laptop: 32
- Netbook: 17
- Smartphone: 7
- Tablet: 24
- None: 1
Appendix L Devices Lost or Stolen

![Bar Chart: Devices Lost or Stolen](chart.png)
Appendix M Employers Allow the Use of Personal Mobile Devices for Work Purposes

Employers Allow the Use of Personal Mobile Devices for Work Purposes

- Yes: 62
- No: 38
Appendix N Employers Have Policies and Procedures in Place for Personal Mobile Device Use

Employers Have Policies and Procedures in Place for Personal Mobile Device Use

- Yes: 72
- No: 28
Appendix O Employer Requires Users to Sign Documentation to Use Personal Devices

**Employer Requires Users to Sign Documentation to Use Personal Devices**

- **Yes**: 35
- **No**: 65