THE UNIVERSITY OF UTAH®

Title: Portable Device Security
Number: G4-004H1
Responsible Office: Information Security and Privacy Office
Last Revision: July 2011

I. OVERVIEW

A. This document is meant to provide procedures, standards, and guidance for the implementation of the University of Utah Information Security Policy – Section H: IT Resource Security.

II. GUIDELINES

A. Protect your portable device

1. A portable device is an amazing tool and can assist you in the workplace and your personal life. By the same token, the information on the device can cause harm to you or your employer. The data stored on the portable device can be used to piece together a very complete picture of who you are, what you do for a living, what you do in your free time, your family, your medical conditions, your finances, etc. We live in a world where information can be exploited and cause harm if you do not properly safeguard your personal data.
2. Maintain physical control of the device.

    a) While it may seem obvious, maintaining physical control may be the best method of protecting your portable device and data that is stored on it. Keep control of your portable device at all times. Do not set it down and walk away or allow anyone else to use it. Just as you would not leave your wallet or purse, don't leave your portable device unattended or in a place where it is likely to be stolen.
    b) Law enforcement agencies view the theft or loss of a portable device or cell phone as a property crime; they do not have the ability to identify where your portable device is, unlike what is portrayed in television and movies. Law enforcement will obtain your information and provide you with a case number. If you have the property number, they may be able to track it in pawn shops or other points of resale, but they may not be able to do more.

3. Do not store restricted or sensitive data on your device.

    a) To help protect against loss, it is very important that sensitive data, such as PHI, is not stored on a portable device. It is against University of Utah policy to do so unless it is approved.
    b) Use remote wipe or remote kill if you lose your device and make the appropriate report to law enforcement agencies.
    c) Many portable devices have the ability to be remotely wiped or killed in the event it is stolen. However, the processes vary by device and provider. Keep the information on how to perform the operations in a separate document not stored on the device. In the event your portable device is lost or stolen, initiate remote wipe feature as quickly as possible. Don't wait: assume the device has been stolen and is no longer under your control to minimize the damage and possible subsequent theft of sensitive data. Be sure you know how to initiate the process before your device is lost.

d) Keep information such as serial number, type of device, and how to initiate remote wipe or kill in a document that is separate from your device. This information can be helpful to law enforcement. You will also want to make sure your information is backed-up because all of your information will be lost during the remote wipe even if your device is found.

e) If your device is lost or stolen, contact your service provider immediately to have the service suspended and the device disabled and wiped remotely. Some smart phones have apps that you can use to wipe the device remotely if it is lost or stolen.

4. Set a password and enable automatic locking on the device

   a) It may be inconvenient, but setting a password to log on and enabling automatic locking of the device when it has not been in use for a period of time are two simple methods of protection. The password and automatic locking can be set by accessing the settings on the device. This does vary by device and you may need to contact your provider or check your instruction manual for further information on how to set the security functions of the device.

5. Use anti-virus software if it is available for your device

   a) There are a variety of applications that can be purchased for your portable device that will protect your device from malware. Your portable device is susceptible to malware in the same way your workstation and laptop are. You should use the same safe security practices on your portable device that you would with your other computing devices. It does not matter what operating system is on the device; all operating systems are susceptible to attack and exploitation.

6. Only download and install software that is from a trusted source

   a) Your portable device has many of the same capabilities that your other computing devices have, for example, the ability to connect with the Internet and interact and download or upload content. Your portable device can be compromised and can have information stolen from it or the device can be rendered useless.

7. Disable Bluetooth discoverable mode after the devices have been connected

   a) Bluetooth, the protocol that allows a portable device to interact with each other, is very useful. A hands-free headset is one example of convenient Bluetooth usage. However, the Bluetooth protocol can be used against you if you allow your device to be discovered by another device. A person can use the Bluetooth protocol to access your device and gather information about you from your contacts, calendar, applications, and/or phone numbers dialed or received. On most portable devices, this feature can be disabled by accessing the settings and turning off discovery mode by Bluetooth. If you have any questions, please consult your device's instruction manual or contact your device provider for further instructions. Please reset the Bluetooth default password as soon as possible.

8. Use VPN connections if the device has VPN capability

    a) If it is available for your device, establish a VPN connection or use a secure protocol such as SSL to transfer sensitive data as it moves back and forth from your device. Remember, your portable device is like any other computer and your data must be protected as it is transmitted.

9. Use accepted procedures to dispose of or retire your device when it is no longer in use.

    a) Your portable device should be decommissioned in the same fashion that you would any computing device. Wipe the hard drive/memory card and remove any restricted or sensitive information.