

PALM BEACH COMMUNITY COLLEGE GUIDELINE

Guide: 6Hx-18-G.001	Category: Standard Practice Guide	Version Date: 08.24.2007
Title: Mobile Device Security and Usage Guideline		Effective Date: 08.24.2007
Originating Unit: Information Technology Security Office		Last Review: 08.24.2007
Review Officer: Chief Information Officer, Anthony Parziale		Next Review: TBD

Overview:

This document describes the security guidelines that the Information Technology Security Office (ITSO) has developed for mobile devices. To protect and preserve the confidentiality, integrity and availability of college information stored on mobile devices such as Blackberry devices, Portable Digital Assistances (PDAs), Smartphones and Laptop computers, appropriate security measures must be established to secure that information from being lost or compromised.

Applies to:

This guideline applies to all campus affiliates. This includes students, faculty, and staff members as well as guest account holders.

Purpose of the Guideline:

The Information Technology Resources and Systems Policy ([Board Policy Number 6Hx-18-1.23](#)) establishes a general policy for the provision, support and security of Information Technology resources. The purpose of this guideline is to establish acceptable practices that support the policy as it applies to mobile devices.

This guideline was established to ensure that Palm Beach Community College has an unambiguous understanding of appropriate procedures and practices. The Information Technology Security Office reserves the right to modify this guideline as necessary. Changes to this guideline will be distributed to associated parties.

Definition:

The Information Technology Security Office defines the following as mobile devices:

- Blackberry devices
- Personal Digital Assistants (PDAs)
- Personal Digital Assistants (PDAs) with Phone
- Smartphones
- Laptop Computers and Tablet PCs
- Flash Memory Drives (i.e. SmartMedia and CompactFlash cards)
- USB port storage devices
- Compact Disk (CD)

- Digital Video Disc or Digital Versatile Disc (DVD)
- Digital tapes

Guideline Statement:

The college strongly recommends the use of general “best practices” when using a mobile device to store college information. Additional measures may be required and appropriate for securing your specific device.

User Responsibilities and Procedures:

College information: It is strongly recommended that unprotected college information should not be stored on or accessed from a mobile device. Following this simple rule can significantly reduce most security risks.

Use encryption: If college information must reside on your mobile device, the best way to protect that information is to encrypt it. This includes college information stored on local and removable storage. With encryption enabled, the data on your device will remain secure in the event that it is lost or stolen.

Secure your mobile device with a password: Due to their popularity and size, physical security for a mobile device can cause major concerns for many colleges and universities. If your mobile device is lost or stolen, your power-on password may be the only thing that stands in the way of someone reading your personal information such as college email and other sensitive data. Here are some tips to follow:

- Choose a strong password. The security of your mobile device is as strong as the password you select. The Information Technology Security Office will soon offer best practice guidelines for selecting a secure password.
- Make an effort to choose effective passwords that is not easily guessed. Although it may be difficult to type in complex passwords on the small keypad or with your stylus, it is in your best interest that you do all that you can do to protect your device. More importantly, the data on that device.
- Similar to your desktop computer, it is recommended that your mobile device is configured to lockout itself after ten to fifteen minutes of non-use. To regain access, the user will have to enter the correct password.

Data transmission: The transmission of all college information transmitted to or from the mobile device should be encrypted. The transfer of college e-mail, for example, should be transmitted via a secure connection or protocol such as SSL (Secure Socket Layer) to ensure end-to-end encryption of all data sent and received. Please note that if you are using WEP (Wireless Equivalent Privacy) on your Wi-Fi mobile device, it is not considered a secure method of protection. Vulnerabilities inherent in WEP can potentially cause serious security risks. The preferred method is to use WPA (Wi-Fi Protected Access).

GUIDELINE

Use antivirus software: Similar to desktop computers, mobile devices can be just as susceptible to viruses. In July of 2004, the first virus specifically designed to target the Pocket PC was released. Created as a proof of concept, the virus dubbed “Dust” was harmless. Shortly after, another Pocket PC virus was released. This time the “Brador” virus was labeled by antivirus companies as a full-scale malicious program that was ready to gain control of your device.

Treat your mobile device as you would treat your desktop computer. Make sure your device is equipped with an updated antivirus before you store college information on it. Currently, a number of vendors offer antivirus solutions for your Pocket PC. Trend Micro, F-Secure, Avast! and Airscanner are a few examples.

Report a lost or stolen device promptly: If your mobile device is lost or stolen report the incident within forty-eight hours from the time that you discover that your device is missing. Please report incidents to either the Information Technology Assistance Center (iTAC) at 561-868-3100, the Telecomm and Network Department at 561-868-3722 or the Information Technology Security Office (ITSO) at 561-868-3262. Lost or stolen mobile devices that contain college information may be subjected to the lost or stolen mobile device mitigation procedures (see the next guideline below).

Be aware of lost or stolen mobile device mitigation procedures: If your mobile device is lost or stolen and stores college information, the college reserves the right to either lockout and/or wipeout the information on the device in order to protect the confidentiality, integrity and availability of the information. If a device is wiped out, all data will be erased including personal settings and information.

Disable options and applications that you do not use: By disabling unused services and applications, you can potentially reduce the security risk to your device. Improperly configured services such as Bluetooth, Infrared (IR), remote access, and other connection functions can leave your device open to unsuspected attacks. In addition, disabling unused services can improve the battery life of your device.

Backup your data on a regular basis: Similar to your desktop computer, your data should be backed up on a regular basis. Most of us can remember the painful lessons learned resulting from a system failure without a backup. If your device is lost or damaged, often times a backup of your data is the only means of restoring that information.

Label your device: Label your mobile device with your contact information such as your name and a telephone number. If your mobile device is lost, having a label affixed to it increases the successful return of the device.

GUIDELINE

Adhere to the college's disposal procedures: When the time comes to sell or dispose your mobile device, removing the batteries will NOT erase your data. Be sure to remove all college information from your device. It is recommended that the mobile device is wiped out to ensure that all college information is removed.

Firewall protection: Whenever available for a mobile device, the college strongly recommends the installation and use of a firewall. Currently, Microsoft Windows and Apple Mac OS X operating systems have built-in firewall software that meets this guideline.

Critical/Security updates: Study shows that most security breaches occur as a result of vulnerabilities found in both operating systems and applications. That is why a procedure should be established and implemented to ensure that critical/security updates relevant to the device and installed application are properly installed and configured. Whenever possible the update process should be set to automatically update the device. In some cases, the device may require restarting in order for the updates to take effect.

Physical protection of mobile devices owned or issued by the college: Reasonable care should be exercised when using the mobile device in public places, meeting rooms, or other unprotected areas to avoid unauthorized access. Also, be aware of your surroundings and avoid accidentally disclosing the information stored on your device. Here are a few simple tips:

- Do not let the mobile device out of your sight.
- All college owned mobile devices should have a permanent property label affixed to it.
- As with all valuable items, your mobile device should be kept out of sight when stored in a locked vehicle.

Contact Information:

Questions, concerns or comments concerning this guideline should be directed to:

Guy J. Albertini

Information Security Manager

Palm Beach Community College

4200 Congress Avenue, ITB 103

Lake Worth, Florida 33461

Tel: 561.868.3262

Fax: 561.868.3259

Revision History:

Guideline Established on: 08.24.2007

Guideline Revised on: TBD