Information Technology

Standard

Mobile Device Security

An increasing number of Central Connecticut State University students and faculty are taking advantage of wireless networks around not only campus but New Britain's hotspots and beyond. As a result more of us are using mobile devices to do our computing. Something that we always need to keep in mind when using these devices is that their blessing is also their curse.

The fact that we can pick up our laptop computers, iPods, Internet enabled mobile phones and PDAs and carry them around with us also leaves the door open for unsavory miscreants to take them while we aren't paying attention. To that end the guidelines below were devised to help all CCSU students, faculty, and staff have some tips to keeping their mobile devices from being carried away.

In addition to the physical security of these mobile devices we also need to be sure that we are keeping the data secure on them. For additional information, click here.

Guidelines for Central Connecticut State University

Effective Date: May 19, 2011

Contents

Summary

These guidelines reflect best practices for securing mobile devices, such as laptop computers, and sensitive information stored on those devices. They were developed by the CCSU Information Technology Department during Spring 2011 and provide interim guidance to CCSU faculty, staff, and students while more comprehensive data classification and security policies and standards are developed.

The major recommendations are:

- Sensitive information, to the greatest extent possible, should not be stored on mobile devices.
- Sensitive information, if stored on mobile devices, should be securely encrypted and a copy-not the only instance of data.
- Sensitive information should always be transmitted in a securely encrypted format.
- Portable devices and storage media with sensitive information should be destroyed or erased so there is no possibility of subsequent data recovery.

Introduction

Numerous security breaches have been reported in recent years, many involving laptops, and many involving sensitive data held by universities (see https://www.privacyrights.org/data-breach). One of the most egregious occurrences was the May 2006 theft of a U.S. Department of Veterans Affairs laptop containing names, Social Security numbers, and dates of birth of 26.5 million veterans and 2.1 million active and reserve service members. Estimates of the number of laptop computers stolen in the U.S. annually range from 600,000 to 750,000 per year and the FBI says 97 percent of those stolen laptops are never recovered.

Mobile devices capable of storing or accessing huge quantities of data are now ubiquitous -- most students, faculty, and staff personally own and use portable data storage devices daily. This unprecedented proliferation implies that almost anyone with access to sensitive data could copy that data to a mobile device and thereby expose sensitive data to additional risks such as theft, loss, unauthorized access, or unintended disclosure.

Compromises of sensitive data can have very serious consequences, such as:

- Criminal, civil, or administrative penalties
- Loss of external funding
- Costs of notifying affected parties
- Costs of remediation for losses, identity theft
- Damaged reputation and loss of public confidence

Consequently, Central Connecticut State University has developed these guidelines to help faculty, staff, and students protect sensitive information on mobile devices.

Definitions

Sensitive information: information whose use is governed by local, state, or federal regulatory control or information that has been deemed non-public, classified, or restricted by the University. Examples of sensitive information include, but are not limited to:

- Student information governed by the federal Family Educational Rights and Privacy Act (FERPA)
- Protected health information as defined by the federal Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Financial information (governed by the Gramm-Leach-Bliley Act, for example).
- Documents or email relating to student, staff or faculty disciplinary proceedings
- Personnel records
- Information covered by confidentiality or non-disclosure agreements

For simplicity, the terms *sensitive information* and *sensitive data* will be used interchangeably.

Mobile device: any electronic device that is portable and contains or has the ability to contain sensitive information or provides the ability to access or transmit sensitive information. Examples of mobile devices include, but are not limited to:

- Laptop or tablet PCs
- Personal digital assistants (PDAs) like various Palm models, the HP iPAQ, etc.
- iPads, iPod Touches
- "Smart" phones such as the BlackBerry, DROID or iPhone
- Portable storage media such as USB flash drives, or SD or CompactFlash memory cards
- Any peripherals connected to a mobile device that may contain sensitive information or allow access to sensitive information, like an external USB hard drive
- Tape, floppy disks, CDs, DVDs, Zip disks and other traditional storage media

Encryption: the process of obscuring information to make it unreadable (i.e., "scrambling" the information) without special knowledge. That special knowledge is often a "key" that is used to decrypt the information so it can be read. One might think of the key as a password used to gain access to the protected information, although that is not technically accurate.

Risks

Risks to sensitive information fall into three broad categories:

- Confidentiality -- disclosure to anyone not authorized to access the data.
- Integrity -- corruption of the data by, for example, unauthorized malicious or accidental changes.
- Availability -- making the data unavailable for its intended use. Examples include partially or fully deleting it, maliciously encrypting it, or preventing access by a denial-of-service attack.

Due to these risks, mobile devices should be considered insecure and therefore require protection according to the following guidelines.

Guidelines

1. **Storing Sensitive Information:** To the greatest extent possible, sensitive information should not be stored on or accessed from mobile devices. This simple rule will do much to reduce risk.

2. **Data Encryption:** If sensitive information must reside on a mobile device, it should be encrypted. The decryption key should be entered manually; this step should not be automated. A means should exist to recover encrypted data when the decryption key is lost.

3. **Multiple Copies of the Data:** Sensitive information residing on mobile devices should not be the only copy. Make sure there is another copy on a more secure device such as a server that is backed up regularly.

4. **Data Transmission:** Any sensitive information transmitted to or from the mobile device should be encrypted and/or transferred with a secure data transfer utility. Use a secure connection or protocol, such as SSL, that guarantees end-to-end encryption of all data sent or received. Devices with wireless capability pose an additional risk of unauthorized access and tampering. These capabilities should be disabled, secured, or protected with a firewall. Note that Wireless Equivalency Privacy (WEP) is inadequate protection for a wireless device transmitting sensitive information.

5. **Data Destruction:** The normal process for deleting data from a hard drive, USB flash drive, cell phone memory, etc., does not completely delete the data. Tools are readily available to easily recover deleted data, and even fragments of files, from these devices. Even if the data is encrypted, it has to be decrypted for use and may therefore exist unknowingly in decrypted form in a temporary file that can be recovered even after deletion. Consequently, sensitive data should be destroyed or erased so there is no possibility of subsequent data recovery.

6. **Password Protection:** Access to the mobile device should be protected by the use of a password that meets Central Connecticut State University's requirements. Click here for more information.

7. **Password Storage:** User IDs (such as your BlueNet account, Banner account) and passwords which allow access to the Central Connecticut State University network or its systems should never be stored in "plain text" (i.e., unencrypted so they can be easily read) on mobile devices.

8. **Password Automation:** On mobile devices, do not automate the supplying of passwords or other security credentials needed to access sensitive data (for example, automatically authenticating to an application or database that contains sensitive information, or having Microsoft Windows store passwords to these systems). Likewise, any software installed on mobile devices that uses script files (a series of commands that are run when the script file is executed) should not contain a user ID or password.

9. **Physical Protection:** Reasonable care should be taken when using mobile devices in public places, meeting rooms, or other unprotected areas to avoid the unauthorized access to or disclosure of the information stored on or accessed by the device. Similar precautions should be taken when using CCSU’s wireless network.

- Special care should be taken in crowds, meetings, and security-screening areas to maintain control over the device. Do not let it out of your sight.
- Mobile devices owned or issued by the University should not be left unattended and, where possible, should be physically locked away or secured.

- Mobile devices should be transported as carry-on luggage whenever traveling by commercial carrier unless the carrier requires otherwise.
- All mobile devices should be kept out of sight and covered when stored in a locked vehicle.
- All University-owned mobile devices should be permanently marked as University property and indicate a method of return in case the device is lost.

10. **Virus Protection:** Any mobile device capable of using antivirus software should have the software installed and configured to provide real-time protection and maintain updated virus signatures. For further information click here.

11. **Security Updates:** A procedure should be established and implemented to ensure that all security patches and updates relevant to the device or installed applications are promptly applied. The patching process should be automated whenever possible. The system should be rebooted immediately after patching if required for the patch to take effect.

12. **Firewall Protection:** Whenever available for a mobile device, firewall software should be installed and used. Microsoft Windows, Apple Mac OS X, and Linux operating systems all have built-in firewall software that meets this guideline.

13. **Disabling Unused Services:** Any services on the mobile device that are not needed, especially those that involve communications like 802.11 wireless, infrared, Bluetooth, remote access, FTP, or other connection functions, should be turned off.

14. **Termination of University Relationship:** All University-owned mobile devices should be returned to Central Connecticut State University immediately upon termination of the assigned user's relationship with the University. If the mobile device contains sensitive information and the device will not be re-used immediately by someone authorized to access the information, the sensitive information should be removed in a manner that prevents recovery.

15. **Mobile Device Sanitization:** Mobile devices and other electronic equipment that contain or access sensitive information, or have been used to access sensitive information in the past, should be processed to ensure all data is permanently removed in a manner that prevents recovery before they are disposed of as surplus equipment or returned to the vendor.

16. **Tracking Software:** All University-owned laptop computers containing sensitive information should use tracking and recovery software, such as "Computrace" by Absolute Software Corp. (www.absolute.com), to aid in the recovery of the laptop if it is stolen or lost. Even laptops that do not contain sensitive information should consider using tracking software.

Communication and Education

Implementing effective mobile device security guidelines requires regular training and communication with the users. Educating users about best practices for protecting the devices and the information they hold can help reduce risks dramatically.

At a minimum, user education programs and policies should:

- Give users some accountability. Users should know the reasons they need to follow agency policies and guidelines, not circumvent or ignore security policies, and observe common sense

- precautions. Users should be made aware that failure to follow University policies may result in disciplinary action.
- Make it clear what is at stake, including the user's own information. Losing a device with sensitive information on it can lead to liability issues, damage the University's reputation, and create other security hazards. Many users also store personal information, such as credit card numbers, on mobile devices, which provides additional incentive to protect the information. Losing a laptop or even a PDA can be extremely disruptive.
- Give users the necessary tools and instruction for securing the devices. Make certain that tools are available and easy to use. For example, passwords and other authentication mechanisms should be easy to configure and use; encryption, if needed, should occur without unnecessary user intervention or decision-making.
- Raise awareness by demonstrating real security risks. Training sessions should show users how susceptible mobile devices are to theft and loss, and the steps they can take to reduce risks. Real-world examples should be used to illustrate risk.
- Notify users of any changes to the policies, guidelines, IT provisioning, and support.

Contact Information

Any questions or comments about these guidelines should be directed to the CCSU Information Technology Help Desk at (860)832-1720 or techsupport@ccsu.edu .

Adapted with permission from the Kansas State University, Mobile Device Security webpage.