

MOBILE DEVICE SECURITY BEST PRACTICES

I. Introduction:

The very features that make mobile computing devices (PDAs, cell phones, and laptop computers) useful (portability, access connectivity, data storage, processing power) also make them a security risk to users and to Purdue University when these devices contain University data. Major features of mobile computing devices that cause a risk to the user and potentially the University include their small size (they can be easily lost, stolen, or misplaced); weak user authentication mechanisms that can be easily compromised or simply disabled by the user; and their ease of interconnectedness.

This document explains general end-user security measures that can be taken on mobile computing devices:

II. Standard:

PDAs

- The PDA should be password protected if that feature is available. The password should block all access to the device until a valid password is enabled.
 - The password used should be as strong a password as technologically possible.
 - Guidance on creating strong passwords can be found on the SecurePurdue website.
- A lost, stolen, misplaced PDA should be reported to your departmental IT department immediately. PDAs should display generic return information, if possible, or be labeled with return information if appropriate.
- University sensitive or restricted data should never be stored on a PDA, unless it can be encrypted.
- Where possible, data transmissions from a PDA should be encrypted.
 - Note that the University's data handling guidelines (referenced below) prohibit the transmission of restricted data via wireless or cellular technology. Encryption is suggested for University sensitive data.
- Wireless access, such as Ethernet, Bluetooth, etc., to the PDA should be disabled when not in use to prevent unauthorized wireless access to the device.
 - In general, keep your wireless connection on hidden mode unless you specifically need to be visible to others.
- Wireless access should be configured to query the user for confirmation before connecting to wireless networks.
 - For example, when Bluetooth is on, select the "check with me before connecting" option to prevent automatic connections with other devices.
- Exercise caution when accepting applications sent via wireless or opening MMS attachments as they may include software harmful to your PDA.

Cell Phones

Cellular devices are not considered secure as they traditionally do not contain options to increase their security. Despite lacking many safeguards, cellular devices today can contain many types of information such as phone numbers and contact information (perhaps contact information that should be kept confidential), calendaring functions, photographs, short notes or voice memos, etc. Security recommendations for the PDA should be followed to the extent that they are technologically possible as a feature of the cell phone.

Laptop Computers

- Standard security protocols, such as those enumerated on the SecurePurdue “Security Checklist” should be followed. This includes ensuring that the laptop computer has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled.
- The laptop computer should be password protected. The password should block all access to the computer until a valid password is enabled.
 - The password used should be a strong password.
 - Guidance on creating strong passwords can be found on the SecurePurdue website.
- A lost, stolen, misplaced University laptop computer should be reported to your departmental IT department immediately.
- The laptop computer should be clearly marked with property or identification tags and the serial numbers should be recorded by the owner.
- Wireless access to the computer should be disabled when not in use to prevent unauthorized wireless access to the computer.
- Wireless access should be configured to query the user for confirmation before connecting to wireless networks.
- When storing or working with sensitive or restricted University data on laptop computers, the University’s data handling guidelines should be followed.
- Encrypt sensitive or restricted information on the laptop computer.
- Don’t use automatic scripts, such as for login.

For All Devices:

- Keep mobile devices with you at all times or store them in a secured location when not in use. Do not leave your mobile devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).

III. Related References

University Data Classification Guidelines

- <http://www.itap.purdue.edu/security/procedures/dataClassif.cfm>

Handling of Printed Information (paper, microfiche, microfilm)

- <http://www.itap.purdue.edu/security/procedures/dataHandling/printedInfo.cfm>

Handling Electronically Stored (Computer-based) Information

- <http://www.itap.purdue.edu/security/procedures/dataHandling/electrStored.cfm>

Handling Electronically Transmitted Information

- <http://www.itap.purdue.edu/security/procedures/dataHandling/electrTrans.cfm>

SecurePurdue website

- www.purdue.edu/SecurePurdue

Issued July 5, 2006 from the Purdue University Security Officer's Group and IT Networks and Security.
Revised October 17, 2008.

Questions about this document can be addressed to itap-securityhelp@purdue.edu.