Acceptable Use Policy

Laptop and Electronic Devices - Safety and Security Guidelines

Effective Date: March 1, 2009
Revised: March 12, 2009

Responsible University Officer: Vice President, Information Technology
Responsible Coordinating Office: Office of Information Technology

Version 1.1

REVISION HISTORY
First Draft: February 26, 2009
Second Draft: March 13, 2009

PURPOSE

The following guidelines have been created to help protect you and the University from accidently losing or exposing sensitive information while using portable electronic devices, including but not limited to notebook computers, personal digital assistants (PDA), cell phones, smart phones, flash drives and other media which contains personal or University data.

It is the responsibility of each employee to follow these guidelines and any other reasonable steps to protect information and equipment.

DEFINITIONS

Sensitive information consists of but is not limited to:

- Identity information (names, addresses, birth dates, id numbers or other information linking back to an individual).
- Transactional data (student records, financial transactions, loan information, etc.).
- Access and authorization information (account names, passwords, etc.).
- Any information which would potentially harm or impact the University’s ability to do business.

GUIDELINES

Social security numbers and credit card numbers must NEVER be stored on local computers, portable electronic devices, or media. Refer to the Remote Access Policy for policies and information on how to access this and other types of information appropriately.

When you first receive a portable electronic device or media make sure that you write down the relevant manufacturer, model, serial number and physical description. Store this information in a secure location separate from the device or media so that you will have it should it be needed later. You should take a
Acceptable Use Policy

copy of this information with you when you travel, but make sure that you keep it in a separate location from the device or media.

You are responsible for maintaining current software versions and updates (i.e. virus software, operating system updates, and application software such as Jenzabar, PowerFaids, Infomaker, etc.), on any laptop in your possession. When reconnecting a laptop to the University’s network, it is imperative you confirm that you are running the latest software versions.

You should always make sure that you have physical possession of any device or media that contains sensitive information when you travel.

• Do not check these devices or media, instead take them as carry-on items.
• When you need to put these devices or media down (while conducting business, eating, riding in a vehicle, etc.) try to keep physical contact if possible and if not ensure that you can visually see the device or media at all times.
• When relinquishing possession of the device or media (while going through airport security, loading bags into a taxi, etc.) make sure that you can visually see the device as much as possible and take possession as soon as possible afterwards.
• When leaving the device or media unattended (such as in a hotel room, conference room, office, etc.) make sure that you secure it in a locked location or leave it with a trusted source. When returning to the room, make sure that you take possession and ensure that no one has removed or accessed the device or media immediately. Never leave the device unattended in an unlocked or unsecured location.
• You should avoid leaving the device or media in a vehicle, but when you need to do so, make sure that you put it out of sight, preferably in the trunk of the vehicle, and that the vehicle is locked. Check to ensure that the device or media is still in the vehicle immediately upon returning.

You should always make sure that you have a current, secure and reliable backup of any sensitive data contained on the device or media.

• It is not possible for the University to centrally backup data contained on flash drives, CDs, PDAs, cell phones, smart phones, etc. at anytime.
• It is not possible for the University to centrally backup data on a notebook when it is not physically on our network.
• You are responsible for making sure that you back up your data frequently and that you store the backups in a secure location separate from the device or media being backed up.
• You must protect the physical access to and contents of these backups with the same level of regard as the originals.

You should encrypt or password-protect any device or media containing sensitive data.

• Every device needs to have a password enabled in order to access the data on the device. You should lock the device so that it requires this password every time you turn it off or put it down.
• If the device or media has the ability to be encrypted, this feature needs to be turned on.
• Passwords should be difficult to crack but easy for you to remember. Good passwords are never recognizable words, phrases, names or dates and should always contain a mixture of upper and
Acceptable Use Policy

lower case letters, numbers and punctuation and should be at least 8 characters long if the device allows. Some devices, such as cell phones or PDAs may limit password length and content. When this is the case, use your best judgment to create as secure a password as possible.

- Passwords should be changed frequently (at least once every 6 months).
- Do not ever store passwords on the device or media or have them written down with the device or media. If you need to write a password down, try writing a hint for yourself rather than the actual password.

If a device or media containing sensitive data is lost or stolen, immediately report the incident to the local authorities and notify the helpdesk with the following information. Delays may increase the risks to the University.

- Device or media manufacturer, model, serial number and physical description.
- What sensitive information is stored on the device or media.
- When, where and under what circumstance the device or media was lost or stolen.

If you have questions or if a device has been lost or stolen, please contact the Helpdesk at:

Phone: (414) 410-4600
Toll-Free: (877) CSU-WOLF [(877) 278-9653]
Fax: (414) 410-4049
E-mail: support@stritch.edu