Security Best Practices

Email Protection

- Never open e-mail attachments or links you don't recognize.
- Never respond to spam.
- Don't provide sensitive or personal information over email where possible.
    - If you need to send sensitive information via email – use encrypted email http://www.utoledo.edu/depts/it/Security/Tools/email_encryption.html
- Before clicking "send", review your message for appropriateness.

Identity Protection

- When transmitting personal information, look for https or secure (key) icon in browser to ensure data is sent encrypted.
- Never send credit card or bank information via email.
- Don't click links to sites where possible. Type them into the browser to ensure you're heading to the right site.
- Remove social security numbers from documents if appropriate and wherever possible.
- If you are unsure if data is sensitive in nature, ask for clarification.
- Avoid sharing sensitive information with unauthorized or untrained staff.
- Sensitive information can only be disclosed for business purposes.
- Complete FERPA training before handling student information.
- Complete HIPAA training before handling patient information.

Account & Password Protection

- Use strong & complex passwords.
- Try to avoid dictionary words.
- Change your password often.
- Don't increment your new password by one character; completely change the password.
- Never re-use an old password.
- Never write down a password.
- Never share accounts.
- Don't give your password to anyone!
- Avoid "remember my password" options
- Make sure no one is looking over your shoulder when you enter your password.
- If you don't have access to a required area, request access, don't use someone else's access.
- You are responsible for all activity associated with your user account.

Software Protection

- Don’t bring software from home without authorization.
- Never turn off Anti-virus or Anti-spyware programs.
- Scan removable media for viruses before using.
- Ensure program and operating system updates are installed regularly.

File Sharing Protection

- File-sharing is not illegal, but sharing copyrighted material is.
- File-sharing software must be authorized before usage.
- Know what your computer is sharing!
- The penalties for sharing copyrighted or inappropriate material are severe.

Storage Protection

- Refrain from storing sensitive information on your University computer or laptop.
- The University provides network storage space for all institutional members and departments (H drives, department shares, etc.).
- If you must store sensitive information on your computer for official business purposes, you must encrypt it. Store backup copies of important files in a safe and secured location.
- Storage must be appropriately wiped or erased before transfer or disposal.
- Avoid using removable media (such as flash drives, USB devices, DVD/CDs, and floppies) unless required. These can easily be lost or stolen.

Display Protection

- Use password-protected screen savers.
- If screen savers are not available, cover up display when not in use.
- Be aware of who can read your display.
- Use power-saving techniques when not in use.
- Be aware of what you display during a presentation.

Printer Protection

- Get your print outs quickly. Anyone can be standing at the printer.
- Don’t print excessive copies, especially if printing isn’t working as expected.
- Ask for assistance if you print to the wrong printer.
- Inform others when they leave print outs at the printer.
- Printers should be in a secured area, or away from public access.
- Dispose of all sensitive print outs in confidential bins.
- You are responsible for everything you print.

Phone & Fax Protection

- Verify the caller.
- Don't disclose sensitive information without approval.
- Be careful of what information is left on other's voicemail.
- Can anyone else hear your conversation?
- Avoid asking for personal or sensitive information, unless required.
- Contact the recipient of a fax prior to transmission.
- Use fax cover sheets on all faxes and mark the transmission as "confidential".
- Remove or mask sensitive information when faxing.
- Know whether the fax machine is in a secured or public area.

Travel Protection

- Don't take patient or sensitive information home!
- Don't leave mobile devices unattended, even for a few minutes.
- Don't leave University equipment unattended in your automobile.
- Secure University equipment when at your personal residence. You are responsible for protecting this equipment!

Physical Protection

- Ask for identification if someone you don't know is in your area.
- Always shut down or log off of any system when not in use.
- Protect your computer from power surges with surge protectors.
- Use locks where possible.
- Lock your doors when you leave your office and never lend your key to anyone.
- Know who has access to your work area and computer.
- Properly dispose or shred all documents that contain sensitive information when they are no longer needed.
- Never leave sensitive information in plain view.
- Never leave valuables unattended (Laptops, PDA's, books, etc.).
- Always secure sensitive documents when not in use.
- Always empty desks and cabinets before transferring ownership.

Responsible Usage of Technology

Review & understand the University's Responsible Use of Information Technology Policy (http://www.utoledo.edu/policies/administration/info_tech/pdfs/3364_65_05.pdf), which includes:

- Complying with All Federal, State, and University laws.
- Use only the UT computing resources that you are authorized to use.
- Respect the privacy of other users and their accounts.
- Respect the finite capacity of UT computing resources.
- Refrain from using UT computing resource for personal commercial purposes or financial gain.
- Computing resources are subject to review and disclosures.
- Refrain from stating or implying that they speak on behalf of the University.

- Using University systems provides your consent to security monitoring, testing and administrative review.
- Users that violate this policy may subject to penalties and disciplinary action, both within and outside of the University.
- Communications made with University resources are generally subject to Ohio's Public Records Statute.

IT Security Policies

IT Security Policies are located at: http://www.utoledo.edu/policies/administration/info_tech/index.html