- Work with your campus technology support organization to make sure that your PC is running current virus software and security updates.
- Don't install file sharing and related applications that expose your PC data to the internet.
- Store university files on university servers, not your C: drive.
- If you access university resources from your home PC; install and maintain current virus software on your PC, and run Microsoft Windows update on a regular basis.
- Never permit others to perform work under your ID.
- When your log in is active on a terminal, take precautions to prevent non-authorized use of your account by another individual.

⁂

Fraud Awareness

- Recognize fraudulent attempts to obtain computer username/password or student/financial information. Never release such information over the phone.
- Use extreme caution in responding to e-mail messages and web sites that ask you to provide or update personally identifiable information.
- Report any suspected attempts to your supervisor.
- Educate all employees, particularly student assistants, about all privacy policies related to their job.

⁂

Indiana University of Pennsylvania
1090 South Drive
109 Clark Hall
Indiana, PA 15705

Information Security Awareness

Training Brochure

IUP is a member of Pennsylvania's State System of Higher Education.

Background

IUP is subject to a variety of information privacy and security laws and regulations including the Family Educational Rights and Privacy Act (also known as FERPA) and the Gramm-Leach-Bliley Act. These acts mandate specific restrictions and safeguards related to access, use, and disclosure of "Restricted Information."

IUP's compliance with these acts is governed by the IUP Information Protection Policy.

All employees must be aware of, and comply with, the IUP Information Protection Policy and the IUP Information Protection Procedures.

⁂

What is "Restricted Information?"

The laws restrict information related to student "Education Records" and "Customer Financial Records."

An "Education Record" is maintained by our institution and contains personally identifiable information about current and former students. Education records include, but are not limited to, the following: University ID, Social Security number, race, religion, gender, ethnicity, financial aid, some health data, grades, test scores, and other academic work completed.

"Customer Financial Records" include personally identifiable information about students, parents, employees, or related third-parties such as bank and credit card account numbers, income and credit histories, and Social Security numbers.

⁂

What are some risks with unauthorized access to Restricted Information?

Unauthorized access to restricted information can lead to identity theft and/or fraud. Following are some examples of events/actions which would permit fraudulent access to such information:

- A computer account with access to various information systems or network files is accessed by unauthorized individuals because a password was shared with other people, written on a post-it by the computer, or easily guessed.
- A user opens a computer virus via an e-mail attachment and the virus randomly distributes sensitive files via e-mail.
- Sensitive paper records are left in easy view where a visitor notes and records personally identifiable information.
- Someone installs file-sharing software on a PC leading to unintended internet exposure of PC and network files.
- A PC containing sensitive data on the C: drive is moved to another office without first removing electronic data stored on the local hard drive.
- Verbally sharing restricted information directly or within earshot of those without authority to receive such information.

⁂

What are some safe practices for information protection?

Computer Passwords

- Never share your password with others. Never post password information at your work area.
- Change your passwords on a regular basis.
- Use passwords that are difficult to guess. Don't use personally identifiable information for a password. Do include a combination of letters and numbers in every password.
- Electronic access for employees should be kept current; access for employees who leave the department/area should be removed immediately.

Physical Access Restrictions

- Store restricted information records in a secure area.
- Protect PC's and laptops from unauthorized access. Log-off your PC when not in use. Use a password protected screen-saver when you are away from your PC.
- Shred printed documents containing restricted information.
- Properly prepare equipment for transfer or surplus by working with your technology support organization to securely eliminate or remove data stored on the equipment.

Safe Computing Practices

- Never open e-mail attachments from a non-trustworthy source.