IT Compliance and Acceptable Use Training

Prepared by:
Christy Bunch (x7297)
John Lugo (x8848)
Matthew McCoin (x7957)
Brian Sheehan (x8967)
Darlene Thompson (x8940)
Introduction
The IT department at TCC would like to ensure that all of its employees are aware of the boundaries that all faculty and staff should abide by when utilizing TCC systems. The College has a Compliance and Acceptable Use policy currently in place, and IT would like to clarify some of that language, provide guidance, and answer questions anyone may have.

Topics that will be covered:
- Compliance as it relates to security and confidentiality
- Acceptable Use as it relates to legal, ethical and reasonable usage
- Wrap up with some administrative items and how to login into TCC systems

Compliance

Passwords
Per the Employee handbook: “Under no conditions should a user make visible, available, or provide his/her password, account, or I.D. to another person.”
By not keeping your password confidential, there is potential for unauthorized intrusion (e.g. system could be hacked, viruses can enter a system/network, malicious emails could be sent, etc). No one should ever ask you for your password – not your supervisor, not the Service Desk, no one. Keep this confidential.

Additionally, each user should create a strong password. Below are some characteristics of strong and weak passwords, and tips on how to create a strong password.

Weak passwords consist of:
Proper names, previously employed passwords or variations of them, words from the dictionary, common character sequences such as ‘123456’ or ‘mar2004,’ derivatives of user-ID, personal details such as variations of your own name, spouse’s/pet’s name, license plate numbers, social security numbers, and birthdates.

Strong passwords are:
At least 6 characters in length
Difficult to guess
Alphabetic and non-alphabetic characters
Upper and lower case letters

Tip: Think of a full sentence. Now take the first letter of each word from that sentence and add a few digits to the end. You now have a unique, difficult-to-crack password.
Example: Coming up with new passwords is sometimes difficult
Password: cuWnPl$d514
TCC passwords should be changed at least every 3 months (e.g. MyTCC, computer login, etc). Put a reminder in your Outlook calendar to change your passwords in case the system does not prompt you to do so. It’s paramount that passwords be changed regularly to avoid chances of hacking by external parties. If you experience problems with your password, contact the IT Service Desk at x2000.

**Security and Confidentiality**

*Confidential information*

Some job functions will require faculty/staff to access and handle sensitive employee and/or student information such as, but not limited to, social security numbers, bank account numbers, and college-wide IDs. Keep in mind that these documents should never be left unattended. If this information must be stored away, be sure they are stored in a secure location. Once there is no longer a need for these documents, ensure they are properly destroyed (e.g. shredded).

*Computer Security*

If you have a personal TCC workstation that can be locked, be sure it is locked every time you step away by pressing “Ctrl + Alt + Delete” and pressing “Enter,” or, if that doesn’t work, press the “Windows” key and “L.” This prevents unauthorized personnel from accessing your system while you are away.

**Acceptable Use**

**Legal and Ethical Usage**

Per the employee handbook: *“Since the use of TCC computing resources are in the public domain, all users are subject to having all of their activities on this system monitored and recorded by college personnel. Any data created or accessed through college resources is considered to be the property of TCC and may be used in disciplinary or college proceedings.”*

*“College computing resources may not be used to violate or be in violation of any municipal, state, or federal law; or to interfere with or disrupt the orderly educational process of TCC; or to exhibit conduct or activity generally considered to be grossly offensive or totally unacceptable to society...”*

See page 19 of the Employee handbook for examples of illegal and unethical usage.

**Reasonable Usage**

Per the employee handbook: *“Unreasonable usage can include unnecessary storage of disk files, careless execution of intensive programs, and the generation of excessive printer output or electronic mail.*

- For multiple copies, use a copy machine, not a printer
- Don’t transfer large amounts of data between computer systems
  - Computing resources are for instructional and research use, not for personal, recreational, or commercial use
- Refrain from overuse of interactive network utilities (Streaming video, etc)”
Computer Usage
All personal TCC desktop workstations have assigned locations and should not be moved without first contacting the IT Service Desk at x2000. Service Desk personnel will provide guidance to the user once contacted.

Laptop computers fall under the same Compliance and Acceptable Use guidelines as desktop computers. If a laptop is damaged, lost or stolen, contact x2000 immediately. If a Service Desk Representative is not available, contact your supervisor for guidance.

Internet Usage
Internet usage should always be appropriate and professional, and all personal internet usage should be kept to a minimum. Visiting inappropriate websites on TCC systems is prohibited.

Hardware/Software
No hardware or software should be added or removed from a user’s system without first contacting the IT Service Desk at x2000; regular computer updates are excluded (e.g. Java updates, Windows updates, etc). Users are prohibited from editing/changing antivirus settings on their system.