PUC PASSWORD POLICY

Passwords are the front line of protection for user accounts. A poorly-chosen password, or one that has ended up in the wrong hands, may compromise PUC's entire network, as well as your personal information, leaving you open to identity theft. Therefore, all PUC constituents (including employees, students, alumni, contractors, consultants, and vendors with access to PUC's systems) are responsible for taking the steps outlined below to secure their passwords. PUC's systems include those that reside at any PUC facility, have access to PUC's network, or store any non-public PUC information.

Protect your passwords and accounts

- *Change* all passwords every 6 months for PUC employees who handle sensitive data and every July 1 for the rest of the employees.
- *Change default* passwords on new systems ASAP.
- *Lock* your computer/screen when you step away from it.
- Watch for *shoulder-surfing* like you would at an ATM.
- Passwords for PUC systems should be *different* than any of your non-PUC passwords.
- When using someone else's computer, use the browser's *private browsing* feature.
- Passwords that provide access to student or employee information must be guarded especially carefully to avoid violating federal mandates such as FERPA and HIPAA.
- Don't *share* passwords, especially via phone/email, even with ITSS personnel.
- Don't store passwords in an insecure way. See recommended password keeping software below.
- Don't leave any password blank, even if it's "protected" by another layer of passwords.
- Don't *recycle* old passwords--assume they've been stolen.
- Don't *trust* any system that can email or show you your password. Make that password *completely* unique.
- Don't *write* any password on a sticky note under the keyboard or in your desk drawer.
- Don't use browser "remember password" feature, a "password-protected" Word or Excel document, or your PDA or phone—these are all insecure.
- It is not safe to reuse an old password for another account (doubly bad).

Suggestions:

- Use a secure password manager such as Lastpass, KeePass, or Roboform (all free). Use a series of phrases with a common theme, the first letters of a phrase, or a combination of several items. For example, take the next line from a favorite poem/song/movie as the theme each quarter.
- Add to a common "stem" to make unique passwords.
- Create your own unique security question instead of selecting one from the predefined list whenever allowed.

Desirable Practice:

- Use a long, easily-remembered phrase, containing an uncommon (or non-English) word, and a punctuation mark or two.
- Make passwords long enough--at least 8 characters.
- Deliberately *misspell* words in your password.
- *Mix* capital and lowercase letters, digits and punctuation.

Examples of Strong Passwords

- 1feliz:)person
- 2B/knot2Bee
- 8:17@CarrmeL

Non-desirable Practice:

- Don't use *public information* (name, login, phone #, birthday, anniversary, pet's name, address, ID#, SSN), including anything you post on social media.
- Don't make your password *a single word* in any language.
- Don't use only digits--too easy to guess.

Examples of Weak Passwords

- Punctiliousness
- 0957865 (PUC ID) or 965-7000
- any published sample passwords (they are public info)

Results of Misuse: Minor infractions of the policy, when accidental, or unintended, will generally be resolved informally by the Information Technology Systems and Services management. Repeated minor infractions or serious misconduct may result in the loss of system access. Additionally, any misuse may be prosecuted under applicable laws. Users may also be held accountable under applicable College policies. Any offense which violates local, state, or federal laws may result in the immediate loss of college computing resource privileges and will be referred to appropriate College offices or law enforcement authorities.

By my use of any PUC computing facilities, I agree to abide by the stated guidelines and policies.

Approved by Administrative Council June 4, 2012