Cal Poly Information Security Awareness and Training

New student employees are required to receive information security awareness training. This document constitutes that training. Please read and keep it on file for reference. Annual follow up training is required and you will be notified when this happens.

As a student employee, you are responsible for ensuring the confidentiality, privacy, appropriate use, and security of data, accounts or equipment that you use in the course of your employment at Cal Poly. All student employees must sign a confidentiality-security agreement acknowledge this responsibility.

Phishing

Phishing emails are designed to make you reveal personal information by pretending to be from a trusted source, e.g., Cal Poly, a bank or online account. They typically ask you to reply or complete an online form with your username and password, financial or other confidential information. Never send a password via email. Never click on a link without verifying with the bank or institution that it is valid. Always treat such emails with suspicion.

Passwords

Use a strong password that is hard to guess. Avoid using the same password for multiple accounts. Your Cal Poly password should never be used elsewhere. Passwords are confidential. Don't share them if you are asked to reveal your password via email, or over the phone, do not give it out! If you suspect your Cal Poly password has been comprised, notify abuse@calpoly.edu and call the ITS Service Desk at once (756-7000).

Safe Computing: Malware, Websites, Email

Always keep your operating systems, browsers and anti-virus software up to date. Use automatic updates and other built-in safety features, such as a firewall, pop-up blockers, etc. Malware can allow an unauthorized third party to monitor or control a computer and often run in the background without your knowledge. Report any unusual symptoms, e.g., slowness, pop-ups, new icons/toolbars.

Malicious websites can infect your computer when you visit them. Avoid unknown sites or sites that anti-virus programs warn you against visiting. Be aware of 'pop-ups' that can contain spyware. Only use known sites that are secure (https) for personal business transactions. Avoid clicking on ads, games, applications and other links on social networks and websites while working. Use available privacy settings and be aware of the risks of sharing too much information on the web.

Be wary of suspicious emails (see phishing above). Do not open email attachments unless you are expecting them and know who they are from. Emails may include viruses or links to unsafe websites. Do not click on links that people send you unless it's a known safe site. Do not send confidential information via email.

Handling Confidential Information

The CSU defines protected information as Level 1 and Level 2. Level 1 data is protected by a variety of laws and regulations. It includes personally identifiable information such as SSN, password, credit card numbers, birthdate, driver's license number, etc. Level 2 data must be protected due to ethical, privacy and proprietary consideration. This includes EmplID, student education records, and employee information such as home address and phone number. Level 3 data is public information.

Learn-by-Doing Security Practices

- Protect your computer against unauthorized access or use, e.g., lock your workstation when you leave, even for a minute
- Protect offices against unauthorized access by people you don't know; report suspicious behavior
- Never disclose protected information over the phone or via email or even in person without proper authorization
- Only use Cal Poly resources and information that you've been authorized to use; do not share your access with others
- Protect your personal devices (smart phones, tablets, laptops) to secure your own confidential data and identity
- Put confidential documents away when not in use
- Be mindful when leaving your desk or having visitors
- Never install software, download files or programs, or make changes to a university computer without proper authorization
- Never attach a jump drive or other 'found' devices to your university computer; such devices may contain protected data or malicious software; report it to your supervisor
- Familiarize yourself with student privacy rights under the Family Educational Rights and Privacy Act of 1974 (FERPA) – http://registrar.calpoly.edu/stu_info/ferpa.htm

Always Remember

- As an employee at Cal Poly, you have access to information which must not be shared
- All users are expected to be familiar with and abide by Cal Poly's Responsible Use Policy, affirmed at least annually when you change your portal password. To review the policy, visit: http://security.calpoly.edu/policies/rup

Seeking Advice and Reporting Violations

- If you are
  - Unclear on if, when and how this applies to you?
  - Unsure about what to do in a given situation?
  - Believe a potential vulnerability may exist?
  - Suspect a potential violation has occurred?
- Then, notify
  - Your manage, supervisor or department head
  - Cal Poly's Information Security Office (security@calpoly.edu)
  - abuse@calpoly.edu

Got Questions?

- Learn more about Information security and safe computing practices at http://security.calpoly.edu