Confidentiality Training

For the Full Confidentiality Training Handbook visit www.sonoma.edu/cms/forms

Overview: SSU must ensure that all Personal Confidential Information (PCI) of its students, employees, and guests is handled and protected correctly according to numerous policies and laws. Below is a listing of some of the policies and laws that handle protecting confidential information and a selected excerpt from the policy or law. Please remember that the information below is not all-encompassing of the laws and policies that govern the handling, storing, and obtaining of PCI. Responsibility is placed upon individual employees of the CSU and SSU to keep up with any changes to these policies.

Protects the privacy of students enrolled in an institution of higher education. Federal regulations prohibit the disclosure of a student’s information to anyone other than the student without the student’s written permission except for the parent of a dependent student. Students must be allowed access to their student records.

“…the right to privacy is a personal and fundamental right…” The Information Practices Act, Section 1798 of the California Civil Code, places specific requirements on state agencies in relation to the collection, use, maintenance and dissemination of information relating to individuals. Careless, accidental or intentional disclosure of information to unauthorized persons can have far-reaching effects, which may result in disciplinary action against those involved (Section 1798.55) and civil action against the CSU.

Title 5, California Code of Regulations - http://ccr.oal.ca.gov/ Personal information should not be transferred out of the CSU unless such transfer is compatible with the disclosed purpose for which it was collected.

The Corporation for Education Network Initiatives in California (CENIC) and Digital California Project (DCP) - Acceptable Use Policy - http://www.cenic.org/calren/aup.html
Requires educational institutions to handle and protect confidential information. Users do not use PCI for profit making activities, partisan politics, or stalking. If policies are not followed or information is used for these activities and not caught, then it is possible the University could lose access to the Internet entirely.

“Wayne Shredding Bill” (State Civil Code 1798.80-82) - http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84
Destroy documents, CDs, erase thumb drives, empty your “Recycle Bin” of any document that may contain PCI that is not being stored for later use in an encrypted format.

Additional Useful links:
Sonoma State University Policy on Personal Confidential Information - http://www.sonoma.edu/uaffairs/policies/pci.htm
Electronic Communications Responsible Use http://www.sonoma.edu/it/policies/respoublesuse.shtml
CSU Data Classification Standard - http://security.sonoma.edu/standards/01-109.shtml

Quick Reminders:

Keyboard Shortcut: ⌘ + ‘L’ ‘Windows’ key and ‘L’ will lock your workstation instantly. Should not replace logging off or shutting down your workstation.

Screen-Saver Password
Macs and PCs alike allow the user to require passwords to be used when exiting a screen-saver.

Work Purposes Only
Only use the information that you have access to for work related activities.

Do Not Share Passwords
Do not tape passwords in plain sight or under a keyboard. Keep them unique from personal ones. Do not let others log into any of your account(s).

Clear Desk
Keep your desk clear of confidential documents. Flip over or cover up any documents when guests enter your workstation.

Use Common Sense
Treat all information, even if you are unsure that it contains PCI, as if it were your own.

Secure Handling of PCI
Never communicate PCI over unsecured channels (applies to traditional or electronic mail and facsimiles). Email is not secure. SSNs, credit card information, performance evaluations, or other highly sensitive information should never be transmitted or stored in an unsecure manner (see CSU Information Security Policy and Data Classification Standard for more detailed information).

Ask
If you ever have any doubt about how to handle confidential data or have questions about any of the policies, ask your appropriate administrator.