



## **PROPERTY, SECURITY, PRIVACY, SEARCHES AND USE POLICY**

All Cal Poly Corporation (CPC) property, including, but not limited to desks, storage areas, work areas, lockers, file cabinets, credenzas, computer systems, office telephones, modems, facsimile machines, duplication machines, and CPC vehicles must be maintained according to this policy. All such areas and items must be kept clean and are to be used only for work purposes, except as provided in this policy. The CPC reserves the right, at all times, and without prior notice, to inspect and search any and all CPC property for the purpose of determining whether this policy or any other CPC policy has been violated, or whether such inspection and investigation is necessary for purposes of promoting safety in the workplace or compliance with state and federal laws. Such inspections may be conducted during or after business hours and in the presence or absence of the employee.

The CPC's computer systems, internet access and other technical resources, including any voice mail or E-mail systems, are provided for use in the pursuit of the CPC's business and are to be reviewed, monitored and used only in that pursuit, except as provided in this policy. As a result, computer data, voice mail and E-mail are readily available to numerous persons. If, during the course of employment, an employee performs or transmits work on the CPC's computer systems or other technical resources, the work may be subject to the investigation, search and review by others in accordance with this policy. In addition, any electronically stored communication that is either sent or received may be retrieved and reviewed where such investigation serves the legitimate business interests and obligations of the CPC or other legal enforcement agency. Such information can be subpoenaed and deleted information can still be retrieved.

Employees must exercise good judgment when using voice-mail, E-mail, internet access and computer systems. The use of E-mail distribution lists should be used for the convenience of the addressees and not for unnecessary or frivolous messages. It is important to carefully assess when it is appropriate to send confidential information and discretion must be used. At all times, the company's voice-mail, E-mail, internet access and computer systems must not be used for the following purposes:

- Accessing, downloading, communicating, and/or distributing any information that is illegal, discriminatory, threatening, harassing, abusive, offensive, unethical, pornographic or immoral in nature.
- Communicating and/or distributing information in conjunction with an employee's outside business endeavors or sales of any product or outside service (home products, cosmetics, etc.).
- Sending messages related to political issues.
- Sending messages or other communications violating a company policy or contrary to supervisory instructions.
- Making personal announcements (items for sale, requests for roommates, etc.)
- Sending or responding to chain letters and inappropriate non-business mass-mailings.

Employees of the CPC are not permitted to use the CPC equipment for non- CPC purposes without permission from the direct supervisor. The CPC recognizes that employees may occasionally find it necessary to use the CPC's telephones, e-mail and internet access for personal business. Such uses must be kept to a minimum and must be made only during break or lunch periods and in adherence to the conditions stated above. All personal, long distance telephone calls must be reported to the CPC in a timely manner and charged to the employee who made the call. The employee has no right of privacy as to any information or file maintained in or on the CPC's property or transmitted or stored through the CPC's computer systems, voice mail, E-mail or other technical resources. User IDs and passwords are confidential and should not be shared with anyone without a legitimate need to know to conduct business (i.e. the system administrator and your supervisor to enable business continuation in unforeseen circumstances). For purposes of inspecting, investigating or searching employee's computerized files or transmissions, voice mail, or E-mail, the CPC may override any applicable passwords or codes in accordance with the best interests of the CPC, its employees, or its clients, customers or visitors. All

bills and other documentation related to the use of the CPC equipment or property are the property of the CPC and may be reviewed and used for purposes that the CPC considers appropriate. Employees are expected to report any unusual or suspicious activity, including possible security breaches or misuse, to management, Human Resources and/or CPC Information Technology (IT).

Employees may access only files or programs, whether computerized or not, that they have permission to enter. Any downloading of programs from the internet or other sources must be authorized by IT. Unauthorized review, duplication, dissemination, removal, damage or alteration of files, passwords, computer systems or programs, or other property of the CPC, or improper use of information or technical resources, may be grounds for disciplinary action, up to and including termination.

Data Security, Confidentiality and Privacy

CPC users are responsible for ensuring the confidentiality and appropriate use of data to which they are given access, ensuring the security of the equipment where such information is held or displayed, ensuring the security of any accounts issued in their name, and abiding by related privacy rights of students, faculty and staff concerning the use and release of personal information, as required by law or existing policies, including Cal Poly's Confidentiality-Security Policy at <http://security.calpoly.edu> and Policy on the Use and Release of Student Information at [www.ess.calpoly.edu/\\_records/stu\\_info/ferpa\\_use.htm](http://www.ess.calpoly.edu/_records/stu_info/ferpa_use.htm).

The CPC is required by State law to disclose any breach of system security to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. If you believe a breach has occurred, you must contact CPC Information Technology as soon as possible.

Cal Poly Information Security Awareness and Training

All employees must receive information security awareness training and are required to complete the on-line California State University (CSU) Information Security Awareness Training. New employees will be notified via email about the Web-based training and how to access the training. Email will be sent from: **Information Security Awareness Training** [<mailto:isat@calpoly.edu>] with a personalized link to the CSU's Web-based information security awareness training tool.

I have read and understand the above policy.

---

Signature

Print Name

Date

J:\HR\USR\WP\FORMS\Privacy Policy.doc Revised 3/10

**RETURN TO: CAL POLY CORPORATION  
HUMAN RESOURCES, BLDG. 15  
Attn: ANGELA BORIN**