UC IRVINE ADMINISTRATIVE POLIVIES AND PROCEDURES

Business and Financial Affairs

Computing and Information Systems

Sec. 714-18: Computer and Network Use Policy

Responsible Administrator: Assistant Vice Chancellor – Information Technology
Revised: September 2011

References / Resources:

- Federal Electronic Communication and Privacy Act of 1986
- California Penal Code, Section 502 (computer crime)
- University of California
    - Electronic Communications Policy
    - Faculty Code of Conduct
    - Guidelines for Sexual Harassment Complaint Resolution
    - Policies Applying to Campus Activities, Organizations, and Students
    - Policy and Guidelines on the Reproduction of Copyrighted Materials for Teaching and Research
- UCI Administrative Policies & Procedures
    - Computing and Information Systems
        - Section 714-15, Policy on Access to University Administrative Information Systems
        - Section 714-16, Procedures for Accessing University Administrative Information Systems
        - Section 714-17, Using University Administrative Information Systems
    - Information Access and Disclosure
        - Section 720-10, Information from Public Records (California Public Records Act) - Guidelines
        - Section 720-11, Privacy of and Access to Information (Excluding Student Records) - Guidelines
        - Section 720-12, Student and Student Applicant Records - Guidelines
    - Electronic Communications
        - Section 800-10, Telecommunications System Guidelines
        - Section 800-12, Data Communication Systems Guidelines
        - Section 800-13, UCInet Guidelines
        - Section 800-15, UCI Guidelines for the UC Electronic Communications Policy

    - Section 800-16, World Wide Web Policy
    - Section 800-17, UCI Implementation Guidelines for Notification in Instances of Security Breaches Involving Personal Information Data
    - Section 800-18, Security Guidelines for Computers and Devices Connected to UCInet
    - Section 800-20, ZotMail Guidelines
- UCI Principles of Community

Contact: Office of Information Technology (OIT) at (949) 824-2222 or oit@uci.edu

The University of California, Irvine (UCI) provides computing resources and worldwide network access to members of the UCI electronic community for legitimate academic and administrative pursuits to communicate and to retrieve and disseminate information. All members of the UCI community (faculty, staff, students, and authorized guests) sharing these resources also share the rights and responsibilities for their use.

A. Rights and Responsibilities

Worldwide, open access electronic communication is a privilege and continued access requires that users act responsibly. Users should be able to trust that the products of their intellectual efforts will be safe from violation, destruction, theft, or other abuse. Users sharing computing resources must respect and value the rights and privacy of others, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. Users are responsible for refraining from acts, intentional or inadvertent, that obstruct the access of others to these resources, waste limited resources, harm resources or information, or violate the rights of others.

To help protect computer and network resources files, users are responsible for setting passwords appropriately, and for keeping passwords confidential by not giving them to another person, and for following other appropriate security procedures. Personal equipment accessing the network must conform to Section 800-18, Security Guidelines for Computers and Devices Connected to UCInet. In particular, personal computers must have current security patches applied and the appropriate security software (e.g., anti-virus protection) properly functioning. Guidance on appropriate security measures may be obtained from OIT or an administrative Information Security Coordinator. Users connecting equipment to the network which threaten the security of the network or other systems by failing to follow this guidance may have their ability to connect equipment to the network suspended.

Most UCI owned computers are under the control of system administrators or managers, who are required to respect the privacy of computer system users. However, they may access user files or suspend services on the systems they manage without notice as required to protect the integrity of computer systems or to examine accounts that are suspected of unauthorized use

or of having been misused, corrupted or damaged. This includes temporarily locking vulnerable accounts, removing hung jobs, reprioritizing resource-intensive jobs, etc.
In addition to campus and UC policies such as the Electronic Communications Policy, many UCI departments have their own computing and networking resources and policies. When accessing computing resources, users are responsible for obeying both the policies described here and relevant departmental policies. Students are also responsible for obeying the policies described in the UC Policies Applying to Campus Activities, Organizations, and Students. In addition, all users are responsible for obeying policies of off-campus network services accessed using UCI resources.

B. Example of Misuse

Examples of misuse include, but are not limited to:

- Knowingly running, installing, or giving to another user, any program on any computer system or network with the intended purpose of damaging or placing excessive load on a computer system or network used by others. This includes, but is not limited to, computer viruses, Trojan horses, worms, bots, spamming, and password cracking programs.
- Attempting to circumvent data protection schemes or uncover security loopholes without prior written consent of the appropriate authority. This includes creating and/or running programs that are designed to identify security loopholes and/or intentionally decrypt secure data.
- Using computers, electronic mail or any other form of computer network based communication to act abusively toward others or to provoke a violent reaction, such as stalking, acts of bigotry, threats of violence, or other hostile or intimidating "fighting words." Such words include those terms widely recognized to victimize or stigmatize individuals on the basis of race, ethnicity, religion, sex, sexual orientation, disability, and other protected characteristics.
- Posting on electronic bulletin boards, Web pages, or any other computer network based dissemination channel, any materials that violate University policy or codes of conduct.
- Attempting to monitor or tamper with another user's electronic communications or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Violating copyright laws or restrictions.
- Violating terms of applicable software licensing agreements.
- Using campus networks to gain, or attempt to gain, unauthorized access to any computer system.

- Using a computer account or obtaining a password without appropriate authorization.
- Facilitating or allowing use of a computer account, password, and/or network access or resources by any unauthorized person.
- Employing, either directly or by implication, a false identity when using an account or other electronic resources. This includes sending unauthorized mail that appears to come from someone else as well as posting or otherwise disseminating materials which misrepresent the identity of the sender.
- Disguising, misrepresenting, or concealing the identity of a computer system connected to the network.
- Performing an act without authorization that will interfere with the normal operation of computers, networks, or peripherals, or will interfere with others' ability to make use of such resources.
- Using an account for any activity that is commercial in nature not related to work at UCI, such as consulting services, typing services, developing software for sale, advertising products, and/or other commercial enterprises for personal financial gain.
- Distributing, posting, or otherwise making available to those not authorized any confidential, sensitive, or private information.

C. Consequences of Misuse

Misuse of computing, networking, or information is unacceptable, and users will be held accountable for their conduct. Serious infractions can result in temporary or permanent loss of computing and/or network privileges and/or Federal or State legal prosecution. Appropriate corrective action or discipline may be taken in conformance with applicable personnel policies, student policies, collective bargaining agreements, and procedures established by the Academic Senate. (In extreme cases, corrective action may include dismissal.) California Penal Code, Section 502 makes certain computer abuses a crime, (such as illegal reproduction of software protected by U. S. copyright law) and penalties can include a fine and/or imprisonment. Files may be subject to search under proper authorization.
Minor infractions of this policy, such as poorly chosen passwords, use of resources in a manner which impedes but does not totally block their use by others are typically handled internally to the department in an informal manner. More serious infractions such as abusive behavior, account invasion or destruction, attempting to circumvent system security, etc. are handled formally through the Office of the Dean of Students or by other appropriate officials.

D. Contact Information

For additional information contact Office of Information Technology (OIT) at (949) 824-2222 or oit@uci.edu.