    - 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

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.

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.

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