

- This includes computers with one or more unique network addresses as well as computers that obtain network addresses on a dynamic basis.

APPENDIX J
UCSC
COMPUTER GUIDELINES

POLICIES FOR USE OF UCSC COMPUTING FACILITIES

It is the policy of the University of California to provide computer resources to students, faculty and staff to be used in ways that are consistent with the university's mission—instruction, research, and public service—and in activities that support that mission, such as administration. These resources include computers, terminals, networks, modems, and printers (see *University of California Electronic Communications Policy, dated August 18, 2005, available on the Web at <http://www.ucop.edu/ucophome/policies/ec/>*).

It is the policy of the university to provide its users with access to local, national, and international sources of information in an atmosphere that encourages sharing of information, access to a rich collection of services, and open and free discussion.

The university expects that its user community will respect the public trust through which these resources have been provided. The work and efforts of the user community should not be subject to unauthorized disclosure, tampering, destruction, theft, harassment, nor should there be a denial of access to resources.

All users of campus computing resources share in the responsibility of protecting the rights of the entire community. All users must guard against abuses of the university's information resources and systems. This includes computers with one or more unique network addresses as well as computers that obtain network addresses on a dynamic basis.

The university has determined that the following list, while not exhaustive, characterizes unacceptable behavior, which may be subject to disciplinary action:

1. use of university facilities in a manner that violates copyrights, patent protections, or license agreements;
2. attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities;
3. any violation of state law as described in the Penal Code. As an example, a copy of Section 502 of the California Penal Code is available separate from this policy statement;
4. any action that invades the privacy of individuals or entities that are the creators, authors, users, or subjects of informational resources;
5. any action that disrupts the availability of a system for others, such as running programs that utilize all system resources and prevent others from making productive use of the system;
6. any use of university computing facilities for personal gain (including advertising, or political purposes without the prior approval of the university);
7. any use of university computing facilities to harass others;

8. attempts to alter damage, delete, destroy or otherwise abuse any computer or network resource.

In addition, the user should be aware of the following policies and expectations:

- The university grants permission to members of its community to use computation resources by issuing individual computer accounts. As a condition of receiving such an account, the user must exercise diligence to keep his or her password as a secret and not disclose it to any other person. Users of shared computers or networks, which connect to the campus network, should not share or transfer their account privileges to any other person.
- The university expects that all those who choose to use our off-campus network connections will understand and honor the policies of those regional and national network organizations to which the university is a party. The use policies for these networks are available separately from this policy statement.
- Campus units that administer computers may also establish guidelines for the appropriate use of their equipment in addition to these campus-wide policies. These guidelines must be consistent with the campus-wide policies.
- When a non-university-owned computer is used on campus, the user must follow all of these campus-wide policies. In addition, if the computer is attached to the campus network¹ it must be registered with the owner's name and contact information, machine manufacturer and model number, location of machine, and the network address of the machine. This registration can be done through divisional computer/network managers or through the Office of Information Technology Services (ITS).

¹This includes computers with one or more unique network addresses as well as computers that obtain network addresses on a dynamic basis.