

**Computing Links**[Policies Home](#)**Search****Computing Services:**

## University Computer and Network User Code of Ethics

The computing systems, networks and associated facilities at California State University, Sacramento (CSUS) are intended to support the University's mission and to enhance the educational environment. All CSUS computer and network users should be aware that they have access to valuable and sensitive resources and that their computer practices can adversely affect others.

In the following, "computer" includes any computer facility operated wholly or partly by CSUS, located on the CSUS campus or offsite facility and/or accessed through CSUS networks; "account" means any account number, access code, userid, username or authorization code for a computer or network, together with its associated password and files; "user" means any person using CSUS computer and/or network facilities; "systems administrator" means the person who grants authorization to use computer and/or network facilities.

The list below constitutes a Computer and Network User Code of Ethics for CSUS . Disciplinary action for violating the Code shall be governed by the applicable provisions of the California Administrative Code or other relevant policy of the University.

1. Users must use only those computer or network accounts which have been authorized for their use. Users are responsible for the use of their computer accounts. They should maintain secure passwords for the accounts issued to them and take precautions against others obtaining access to their computer resources. This obligation to maintain a secure environment applies particularly to users who are responsible for confidential information.
2. Users must not share their account with others. With few exceptions, accounts are issued to individuals for specific purposes and are not to be shared.
3. Users must use computing facilities and services only for the purpose for which they were authorized. Specifically, University research and instructional accounts must not be used for private consulting or sold to other individuals. Use of any part of the computing and/or networking resources for direct personal financial gain (except for appropriate contract and external accounts) or to provide free resources for unauthorized purposes is not allowed.
4. Users must not attempt to access or copy the programs and information belonging to other users or to the University unless they have authorization to do so. Programs, data, and information may not be moved from one computer or network system to another without proper authorization.
5. Users must not attempt to interfere with the normal operation of the system.
6. Users must not attempt to encroach on others' use of computing and/or networking facilities or to deprive them of resources.
7. Users must not attempt to subvert the restrictions associated with their computer accounts.
8. Users must not use computing and/or networking resources to send obscene, vulgar or harassing messages.
9. Users must not attempt unauthorized access of computer installations outside CSUS using CSUS computers or networking facilities.

Although system administrators may attempt to provide and preserve security of files, accounts, passwords and programs, it is possible that security can be breached through action or causes beyond reasonable control. Users are therefore urged to safeguard data and to take full advantage of the file security mechanism built into systems. System administrators of shared facilities have a responsibility to inform users of their obligations in the use of these systems.

For further information, please see the following documents:

- [University Computing and Telecommunications Security Policy](#)
- [Computer and Network Password Guidelines](#)

Last Updated: January 3, 2008

[IRT](#) | California State University, Sacramento | 6000 J Street | Sacramento, CA 95819 | (916) 278-7337