33.04.99.W1/PR   Rules for Responsible Information Technology Usage
Approved July 5, 2004
Supplements System Policy 33.04 and the TAMUS Ethics Policy 07.01

1.   GENERAL

1.1   West Texas A&M University recognizes the importance of information technology to students, faculty and staff in scholarly pursuits, professional development, service activities, personal development and every day work and class related activities.

1.2   Use of these resources and facilities is a privilege and requires that individual users act in compliance with University Rules. The University provides users with an account that permits use of the computing resources and facilities within guidelines established by West Texas A&M University. Users must respect the integrity of computing resources and facilities, respect the rights of other users, and comply with all relevant laws (local, state, federal, and international), University Rules, System Regulations and contractual agreements. The University reserves the right to limit, restrict, or deny computing privileges and access to its information resources for those who violate University policies and/or laws.

1.3   As an institution of higher learning, West Texas A&M University encourages, supports, and protects freedom of expression and an open environment to pursue scholarly inquiry and to share information. Access to networked computer information in general and to the Internet, in particular, supports the academic community by providing a link to electronic information in a variety of formats and covering all academic disciplines. As with any resource, it is possible to misuse computing resources and facilities and abuse access to the Internet. The following statements address, in general terms, West Texas A&M University's philosophy about computing use. Additional information can be found in The Texas A&M University System Policies and Regulations.

2.   FREEDOM OF EXPRESSION

Censorship is not compatible with the goals of West Texas A&M University. However, some computers may be dedicated to specific research or teaching missions that limit their use. The University should not limit access to any information due to its content when it meets the standard of legality. Forms of expression that are not protected by the First Amendment and therefore may be subject to censorship by the University include: obscene material, child pornography, or other violations of the law.

3.   PRIVACY

The general right to privacy is extended to the electronic environment to the extent possible. Privacy is mitigated by the Texas Public Information Act, administrative review, computer system administration, security and audits. Contents of electronic

files will be examined or disclosed only when authorized by their owners, approved by an appropriate University official, or required by law.

4.   INTELLECTUAL PROPERTY

All members of the University community should be aware that property laws apply to the electronic environment. Users should assume that works communicated through a network are subject to copyright unless specifically stated otherwise. Utilization of any electronically transmitted information should be within the "fair use" principle unless permission of the author is obtained.

5.   CRIMINAL AND ILLEGAL ACTS

Computing resources of the University, which include the hardware, software, and network environment, shall not be used for illegal activities. Any such use of these resources will be dealt with by the appropriate University authorities and/or other legal and law enforcement agencies. Criminal and illegal use may involve unauthorized access, intentional corruption or misuse of computing resources, theft, obscenity, child pornography and sexual harassment.

6.   AUTHORIZED USE

Computing resources are provided by the University to accomplish tasks related to the University's mission. Computing resources may not be used for commercial activities or illegal activities. Incidental personal use of computing resources by employees is governed by the Texas A&M University System Ethics Policy.

7.   INDIVIDUAL RESPONSIBILITY FOR USE OF COMPUTING RESOURCES

7.1   It is expected that all members of the University community will use these resources and facilities in accordance with University rules and System policies. Failure to fulfill these responsibilities may lead to the cancellation of computer account(s), disciplinary action by the University, and/or referral to legal and law enforcement agencies. Individuals using the University's computing resources or facilities are required to:

7.1.1   Use University computing resources and facilities (mainframe computers, computer work stations, computer networks, hardware, software, and computer accounts) responsibly, respecting the rights of other computer users and complying with laws, license agreements, and contracts.

7.1.2   Use communal resources with respect for others. Disruptive mailings and print jobs, tying up workstations by downloading music or movies, and other disproportionate uses of computing facilities prevent others from using these resources.

7.1.3 Limit use of University computing accounts to the intended purpose. Use of University-owned computers (offices and computer labs) shall be limited to University related business or incidental personal use. As defined in the TAMUS Ethics Policy, employees may use computing resources for personal reasons as long as that use does not result in additional costs or damage to the University and generally does not hinder the day-to-day operation of University offices and facilities. Use of computing resources for commercial purposes or personal gain is prohibited.

7.1.4 Protect passwords and use of accounts. Individuals should not share their user accounts and/or passwords with anyone. Confidential information contained on various computers should not be shared with others except when that person is authorized to know such information.

7.1.5 Report improper use of computing resources and facilities. Improper use of computing resources and facilities may include:

1. **breach of security -** unauthorized access to computing resources, release of password or other confidential information on computer security
2. **harmful access -** creating a computer malfunction or interruption of operation alteration, damage, or destruction of data, injection of a computer virus
3. **invasion of privacy -** reading files without authorization

7.1.6 Comply with requests from the Division of Information Technology about computing. Non-university owned hardware or software are not allowed on campus networks and computers.

7.1.7 Report any incidents of harassment using University computing resources and facilities. It may be harassment if:

1. the behavior is unwelcome; and
2. the behavior interferes with your ability, or the ability of others to work or study; and
3. the behavior creates an intimidating, hostile, or offensive environment.

7.1.8 Respect the forum (talk groups, bulletin boards, public computing facilities) when communicating ideas to others via University computing facilities and resources (includes access to the Internet). All communications should reflect high ethical standards and mutual respect and civility.

CONTACT FOR INTERPRETATION: Assistant to the Chief Information Officer