



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

A. Introduction

The University of Texas - Pan American (UTPA) computing and information technology resources (computing resources) support the University's missions of teaching, research, learning and service. The shared use of these resources requires legal and ethical behavior by all members of the university community. Laws, standards, policies, contracts, mission requirements, and community ethical and moral norms place limits on what is permissible on a university campus. Activities that are technically feasible to perform may in fact be prohibited.

1. Purpose

- a. The purpose of this policy is to provide users of UTPA computing resources with basic knowledge and general guidance for proper, fair, efficient, and effective use of those resources. This policy complies with existing University of Texas System and State of Texas policies and standards. For issues not addressed by this document, refer to applicable University of Texas System or State of Texas policies and standards.
- b. Detailed information about the use of computing resources on campus may be addressed in guidelines consistent with this policy and with laws that protect individual rights. Such detailed information is available in the Employee Information Security Manual, Student Computer Lab Handbooks, and on official WEB pages of campus computer and information service departments.
- c. University departments are encouraged to develop and implement pertinent policies and procedures concerning the use of their computing resources, insuring their policies and procedures comply with this and other University policies.

2. Scope

- a. This policy applies to all users of UTPA computing resources, including, university administrators, faculty, staff, students, and all others authorized to use such resources through their association with The University. This policy applies to all methods of accessing these resources including, but not limited to, campus network connections in academic units, administrative offices, academic laboratories, The University Library, and student dormitories, and remote network connections via dial-up, telnet, internet, and other access means. Violations of this policy will lead to disciplinary action.



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

3. Legal Requirements

- a. Many laws affect the way computing resources may be used. These include, but are not limited to: Libel laws; Privacy laws; Intellectual Property laws (A. copyright and trademark laws); Laws that criminalize obscenity and child pornography; Computer Fraud and Abuse Act (prohibits unauthorized access); Regents' Rules regarding publishing and public speech; Regents' Rules regarding ethical behavior; Contract law (software licenses); Laws limiting the use of State resources (no personal financial or other gain).
- b. Laws, such as the First Amendment to the U.S. Constitution and other federal and state laws that protect individual rights place limits on the University's management and on the user community's use of computing resources. Ethical and technical requirements also influence the University's computing environment.

B. Activities

1. Ethical and Responsible Use

- a. Because university computing resources are limited, The University and its users share responsibility for proper management and use of these resources to insure their availability to support the University's missions.
- b. University Responsibility: The University is responsible for securing its computing resources to a reasonable and economical degree against failure, hazards, loss of data, unauthorized access and/or abuse and to insure computing resources are available for all authorized and legitimate use. This responsibility includes informing users of expected standards of conduct and the consequences for not adhering to them.
- c. User Responsibility: Each user is responsible for their actions in the use of computing resources and for reading, understanding, and adhering to this and other policies concerning the proper use of university computing resources including any laboratory or department-specific policies. Users should consult the Computer Center, Academic Laboratory Coordinator(s), or responsible computing resource manager for details on the policies relevant to a specific resource.

2. Appropriate Use of Copyrighted Material and Trademarks

- a. The University Policy on the Use of Copyrighted Materials requires all members of the University community to follow copyright law. The UT System provides references explaining Fair Use of Copyrighted Materials and how to respond to



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

complaints alleging infringement. Users are expected to understand this law and apply it. Users who infringe others' rights are subject to termination of their accounts and disciplinary action. Similarly, all members of the University community must respect others' rights in their trade and service marks. Such marks may only be used with the permission of the owner. This applies to University (UT System Board of Regents') marks also.

- b. Use of University name in personal home pages: Faculty, staff and students may not use the University name in their home pages in any way that implies University endorsement of other organizations, products or services. They may not use University logos and trademarks, or the University seal. Permission to use the University name, logos, and seal in any way is granted by the Office of University Relations only. Responsibility for the content of users' home pages resides solely with the author(s). The views and opinions expressed by students are strictly the views and opinions of the authors and do not constitute the official sanction of the University.

3. Authentication/Security

- a. Access to computing resources is often restricted in accordance with the purpose to which the resource is dedicated. No one may access a resource without authorization or use it for purposes beyond the scope of authorization. Users may not share an account, a password or other authentication device.
- b. With proper safeguards University offices and departments may conduct official business utilizing processes that establish identity by means of authentication systems approved by the appropriate office.
- c. User Accounts: The University owns all user accounts and grants a specific user, and only that user, the privilege of using it. In most cases, it means users are granted a limited right to use the account. Access to computing resources is available to designated persons subject to user affiliation to the University and/or existing interagency agreements with the University. All access requires positive verification of a user's identity and affiliation to the University at the time of access request and completion of compliance agreement before any access is granted.
- d. User Monitoring: The University will not monitor user transactions or the contents of user files as a routine matter. However, the University reserves the right to monitor, access, retrieve, read, and/or disclose user communications at any time, including but not limited to, when: (a) a legitimate State or University need exists that cannot be satisfied by other means, (b) the involved party is unavailable and timing is critical to a State or University activity, (c) there is reasonable cause to



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

suspect criminal activity or policy violation, or (d) monitoring is required by law, regulation, or third-party agreement. See also C-2-c and C-2-d below.

4. Political Activities

- a. An employee of The University may engage in political activities, but not during work-time or with the use of state resources. Students are similarly restricted from using state resources when they engage in political activity.
- b. Incidental personal use of such resources as email and internet access is NOT considered a misuse of those resources

5. Advertising

- a. The Regents' "solicitation" rules apply to advertising on University property including its computing resources. Since commercial activities can detract from or distort the University's primary mission of teaching, research and service, solicitation is generally prohibited. The Regents' Rules spell out specific narrow exceptions from the general rule for activities that *clearly relate* to the University's mission. As a general rule, an activity that would not further our mission except for the revenue it produces will not be considered a related activity.
- b. Permission to place advertising on any University computing resource must be approved by the appropriate office, and only when it fits within one of the specific exceptions in the Regents' Rules where there is a strong likelihood that the activity will significantly benefit the University as a whole.

C. Resources

1. World Wide Web

- a. Publishing Guidelines
 - 1) Web publishers are responsible for the content of the pages they publish and are expected to abide by the highest standards of quality and responsibility. These responsibilities apply to all publishers, whether they are colleges, departments, student or employee organizations, or individuals. A web page should clearly identify the person or unit responsible for its creation and maintenance.
- b. Personal Pages/Course Pages



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

- 1) Personal pages at The University are easy to identify as most follow the worldwide convention of having a tilde (~) in the URL. To assist others in distinguishing personal pages from official University web pages, owners of personal pages should include a link to a Personal Page Disclaimer in a page footer.
- 2) Faculty, staff, and students are advised to consider the public nature of information they disseminate on the Internet through the World Wide Web. Information in a home page is published and available to everyone who can get to the World Wide Web. Users must not assume that their information is restricted to the campus community.
- 3) Faculty, staff, and student users may not use home pages for commercial activity. This includes but is not limited to running any sort of private business through a home page. Users may not use home pages for fund-raising or advertising for commercial or non-commercial organizations, except for University-related organizations and University-related events.

2. Email, including list servers, newsgroups, and Internet Relay Chat

- a. Members of the university community are encouraged to use email for University-related activities and to facilitate the efficient exchange of useful information. Access to email is a privilege and certain responsibilities accompany that privilege.
- b. Ethical Use of Email: Users of email are expected to be ethical and responsible in their use including making efficient use of computing resources and avoiding wasteful and disruptive activities such as sending chain letters, broadcast messages or other unwanted material. An unwanted message may be perceived by the recipient as abusive, threatening, or harassing, especially if repeated. Such communications may be a serious breach of University policies and law.
- c. Restraint or Monitoring of Content: The University will not impose any restraints on, nor make any effort to monitor the content of, communications other than those imposed by applicable Federal, State or local laws, including laws regarding the right to privacy and laws which prohibit defamatory material. University computing resources users are advised that their communications are subject to such laws and that the consequences of violations can be severe. See also B-3-d above.
- d. No Expectation of Privacy: It is not technologically feasible for the University to guarantee the privacy of electronic communications, therefore users do not have a reasonable expectation of privacy for their electronic communications. Users should



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, modified, and stored by others. Furthermore, electronic communications may be accessed by others as authorized under University of Texas System and University of Texas - Pan American policies. The electronic mail of state employees is subject to the Open Records Act in the same way that printed or typed letters and memos are. See also B-3-d above.

- e. Access for Retirees and Alumni: Computing resources and Internet access for alumni and/or retirees may be provided so long as the recipients have clear ties to the institution and the cost of providing services is recovered.

3. All Servers

- a. All servers (in the University domain/using a university internet address) must be operated in accordance with this policy and any related server security policies. Servers are permitted only to the extent that they do not use more than a fair share of the available institutional resources or violate laws such as the Copyright Act. While University policy permits a dormitory resident, a visitor to the library, or a student dialing into the network from home to connect their own computer to the University's network, where the computer is run as a server the user bears the additional burden of appropriate and secure server management.
- b. All servers connected to the University's network must be used only in ways that: 1) comply with this policy and related server security policies; 2) do not impede the use by other legitimate users of University computing resources and networks; 3) do not violate criminal or civil law.

D. Records

1. Academic Advising/Student Records

- a. Most student educational records are considered confidential under a special federal law (Family Educational Rights and Privacy Act of 1974 - FERPA). The University cannot permit access to or release of protected student records without the student's consent. Some access and release of protected records is permitted under the law such as directory information which is a portion of the student record not protected from disclosure unless the student explicitly asks that it be kept private. Directory information includes such things as name, address, email address, major area of study and degrees granted. Details of the law are summarized in UT Pan American's undergraduate and graduate catalogs.



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

- b. All employees, whether user, manager, or custodian of user files must not abuse the trust placed upon them regarding faculty, staff, and student information. It is a violation of University policy for any employee, including system administrators and managers, to use the computing systems to satisfy idle curiosity about the affairs of others, with no substantial purpose for obtaining access to the files or communications of others. Employees who obtain access to personal information will disclose this information only in the process of conducting legitimate business of the University and only as specifically authorized.

2. File Retention (Document Destruction)

- a. As a State institution, the University must maintain its records in accordance with record retention schedules filed with the Texas State Library, and approved by the State Archives Commission and State Auditor's Office. These schedules apply to electronic documents in the same way they apply to paper documents. Records should be kept only so long as is necessary.
- b. Employees must familiarize themselves with the retention periods that apply to the kinds of information they create or receive. State retention schedules give the University the right to dispose of University records, and the responsibility to insure employees follow them and destroy records in a systematic way. It is not in the University's best interests to keep information forever or to dispose of information that should have been kept.
- c. To prevent accidental loss, all files and messages stored on University systems are routinely copied to tape, disk, and other storage media. This means that information stored on University information systems -- even if a user has specifically deleted it -- is often recoverable and may be examined at a later date by systems administrators and others designated by management. The owner for each system has specific policies in place for backup and protection of user data. Users are responsible for knowing the policies in effect on the systems they use and for assessing whether they are appropriate for the user's data.

E. Related Laws, Guidelines, and Policies.

1. Family Educational Rights and Privacy Act
2. UT System Policy for the Use and Protection of Information Resources (BPM 53)
3. UT System Ethics Policy and Guidelines
4. Regents Rules and Regulations



Handbook of Operating Procedures

Section: 8.9.2
Originally Approved: 03/10/00
Last Amended: 03/22/02

COMPUTER AND INFORMATION TECHNOLOGY USE POLICY

5. Texas Computer Crimes Statue (SECTION 1. Title 7, Chapter 33, Texas Penal Code)
6. Political Activities by State Employees (A. Government Code, Chapter 556)
7. Appropriation Act Rider - Article IX, Section 5: Political Aid and Legislative Influence Prohibited

F. Policy Review

This policy should be reviewed every five years by the University's designated Information Resources Manager with the advice of campus technology management and committees and councils concerned with technology issues.