

Procedure No. 27.99.99.T1.01 (Effective 5/16/03)

Computer Use

PROCEDURE: Tarleton State University provides each of its students, faculty and staff with one or more computer accounts (user-IDs) that permit use of the university's technology resources. Use of these resources is a privilege, not a right. When using these resources, individuals agree to abide by the applicable directives of the university, as well as federal, state and local laws. The university reserves the right to limit, restrict or deny access to its technology resources, as well as to take disciplinary and/or legal action against anyone in violation of these directives or applicable law.

Applicable Directives

Users of the university's technology resources must not only comply with the directives outlined in this document but also with other university rules and procedures. The Texas A&M University System's (TAMUS) policies and regulations against harassment, plagiarism, and unethical conduct also apply as well as any procedures that govern computer usage at a particular facility on campus.

Laws that apply to users of the university's technology resources include, but are not limited to, federal, state and local laws pertaining to theft, copyright infringement, insertion of viruses into computer systems, and other computer-related crimes.

These directives apply to all university technology resources, including but not limited to single-user microcomputers, multi-user servers and mainframes, and the network infrastructure, and includes resources administered centrally or within a department. Technology resources include hardware, software, communications networks, electronic storage media, and documentation. Data includes all files, regardless of size or storage media, including e-mail messages, system logs, and software (commercial or locally developed).

General Philosophy on Computer Use and Security

Authorized Use: Tarleton State University provides technology resources for the purpose of accomplishing tasks related to the university's mission.

Some computers, networks, and software located on the university campus may be dedicated for specific research, teaching missions or purposes that limit their use or access.

Students who have paid their fees will be allowed to use the university's technology resources for school-related and personal purposes, subject to these directives, other applicable rules, and state and federal law; and as long as personal use does not result in any additional costs to the university. Students who have graduated or who leave the university for any reason will have their computer accounts terminated. Continuing students enrolled for the spring semester who do not graduate may retain their computer account(s) during the summer.

An employee of the university shall be allowed to use technology resources in accordance with these directives, and other applicable rules. Incidental personal use of technology resources by employees is permitted, subject to review and reasonable restrictions by the employee's supervisor; adherence to applicable rules, regulations, and policies and state and federal law; and

as long as such usage does not interfere with the employee's accomplishment of his or her duties and does not result in any additional costs to the university. When an employee terminates employment, his or her access to the university's technology resources will be terminated immediately.

Privacy: Users of the university's computer systems should be aware that computer use may be subject to:

1. review or disclosure in accordance with the Texas Public Information Act and other laws;
2. administrative review of computer use for security purposes, for investigation of policy or legal compliance, or during computer system maintenance; and
3. audit as required to protect the reasonable interests of the university and other users of the computer system.

In using the university's computer systems, users expressly consent to university monitoring for these purposes and is advised that if such monitoring reveals possible evidence of criminal activity, the university administration may provide that evidence to law enforcement officials. Further, all users should understand that the university is unable to guarantee the protection of electronic files, data or e-mails from unauthorized or inappropriate access.

Intellectual Property: All members of the university community should be aware that intellectual property laws extend to the electronic environment. Users should assume that works communicated through the computer network are subject to copyright laws, unless specifically stated otherwise.

Valuable assets: Technology resources and data are considered valuable assets of the university. Further, computer software purchased or leased by the university is the property of the university or the company from whom it is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these technology resources may constitute a computer-related crime, punishable under Texas statutes and federal laws. University technology resources may not be transported without appropriate authorization.

Users Must:

1. Know and obey the specific policies established for the systems and networks they access.
2. Comply with laws, rules, policies, regulations, procedures, license agreements, and contracts that pertain to and limit the use of the university's technology resources.
3. Use the university technology resources responsibly, respecting the needs of other computer users. All users must manage their e-mail accounts to remain within the university stipulated disk quotas. Users should maintain the secrecy of their account name(s) and password(s).
4. Report any observed or known misuse of technology resources or violations of these regulations to a computer lab supervisor, the help desk, a department head, or the Office of Information Resources.
5. Comply with all reasonable requests and instructions from the computer system operators/administrators.
6. Reflect high ethical standards, mutual respect and civility when communicating with others via the university computer system.

- a. Respect the rights of others to freedom from harassment or intimidation.
- b. Be polite and courteous.
- c. Use caution when giving out addresses or phone numbers (both yours and others).
- d. Practice network etiquette when communicating electronically.
7. Comply when asked to discontinue using wireless devices (such as network LAN devices, cordless telephones, cameras, and audio speakers) using 2.4 GHz frequency band if they cause interference with the wireless network services.

Users Must NOT:

1. Commit illegal acts. University technology resources are not to be used in support of or for illegal activities. Any such use will be reported and dealt with by the appropriate university authorities and/or law enforcement agencies. Illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of technology resources, theft, obscenity, and child pornography.
2. Use the university computer system in a manner that violates other rules, procedures, regulations, and policies such as racial, ethnic, religious, sexual or other forms of harassment or intimidation.
3. Use the university's computer system for the transmission of commercial or personal advertisements, solicitations, promotions, or political material without approval obtained through university-established channels.
 - a. A bulletin board is currently provided for personal use.
 - b. The appropriate vice president may grant approval for faculty and staff and the Dean of Student Life may grant approval for students.
4. Use the distribution lists for faculty, staff and students to send information other than official university business. A brief description of the guidelines for use of distribution lists is included in this document.
5. Distribute copyrighted materials without providing written permission from the author to the university or determining that use of the materials complies with copyright laws.
6. Duplicate commercial software. All commercial software is covered by a license agreement or copyright of some form.
7. Misrepresent one's identity via electronic or any other form of communication. Use of someone else's access information is prohibited.
8. Abuse technology resources including, but not limited to:
 - a. endangering or damaging specific computer software, hardware, program, network or the system as a whole, whether located on campus or elsewhere on the global internet;
 - b. creating or purposefully allowing a computer malfunction or interruption of operation; e.g., injection of a computer virus on to the computer system;
 - c. disrupting university operations or the operations of outside entities (Applications that use an unusually large portion of the bandwidth for extended periods of time and applications designed to send repeated email messages or mass email messages are not permitted.);
 - d. printing that ties up technology resources for an unreasonable time period; and
 - e. failing to adhere to applicable time limits for particular computer facilities.
 - f. failure to adhere to the [Wireless Airspace Guidelines](#)
9. Breach security systems.
 - a. Failing to protect a password or account from unauthorized use.
 - b. Permitting someone to use another's computer account, or using someone else's computer

account. (The Executive Director of Information Resources will develop guidelines to govern any exceptions to this rule.)

c. Using, accessing, duplicating, disclosing, altering, damaging, or destroying data contained on any electronic file, program, network,

or university hardware or software without authorization.

d. Accessing any systems, software, or data for which you are not authorized. Sharing access to copyrighted software or other copyrighted material on the network is prohibited. University specific network resources or network resources obtained commercially by the university may not be transmitted outside of the university community.

e. Attempting to circumvent, assisting someone else or requesting that someone else circumvent any security measure or administrative access control that pertains to university technology resources.

10. Modify or extend the network wiring and/or services beyond the area of its intended use. This applies to all network wiring, hardware, and in-room jacks.

a. Using hub/hublet is prohibited unless provided by Information Resources.

b. Providing intranet or internet access to anyone outside of the university community for any purpose is prohibited. Under no circumstances may users give others access to the university systems.

c. Providing network services from user computers is prohibited. Users who have an academic need to provide such services from their personal computer must present a written request to Information Resources and be granted permission prior to activating any such services on the network.

11. Use the name "Tarleton State University" in any form or use any symbol, logo, or graphic associated with Tarleton State University for any purpose. An exception to these requirements is when one is engaged in duties authorized by your position as an employee of the university or, if a student, engaged in university sanctioned academic or extracurricular activities. See the Office of Publications and Graphic Design for questions concerning use of these items.

Sanctions for Failure to Adhere to these Directives

Alleged violations of these directives shall be processed according to the established procedures outlined in the Tarleton State University Faculty Handbook, the Staff Handbook and the Student Handbook. The university treats access and use violations of computing facilities, equipment, software, information resources, networks, or privileges seriously. Abuse may subject the offender to prosecution under appropriate laws. The Dean of Student Life will process student violations, and faculty and staff violations will be processed using the appropriate lines of authority.

It is important to note that failure to adhere to these directives may lead to the cancellation of a user's computer account(s), suspension from the university, dismissal, or other disciplinary action by the university, as well as referral to legal and law enforcement agencies. A user's computer account(s) may be suspended temporarily until the violation has been processed or permanently at the discretion of the appropriate university official.

Responsibilities of Deans, Department Heads, and Supervisors

1. Ensure that employees within a department comply with these procedures and other applicable university rules and are given reasonable opportunities to attend appropriate training.

2. Promptly inform the Office of Information Resources when employees have been terminated

so that the terminated employee's access to university technology resources may be discontinued.
3. Promptly report ongoing or serious problems regarding computer use to the Office of Information Resources.

Auditor Access of University Computing Resources

There will be occasions when auditors require access to university technology resources and data files. The access will be permitted in accordance with these guidelines:

Internal Auditors from The Texas A&M University System:

- Shall be allowed access to all university activities, records, property, and employees in the performance of their duties.

State and Federal Auditors:

- Will be granted access to university technology resources and data files on an as needed basis, as approved by the Office of Information Resources and the Office of General Counsel, The Texas A&M University System.

Laws That Pertain To Computer Usage:

Texas Administrative Code, 201.13(b): Information Security Standards

State of Texas law that sets forth the requirements state entities must follow regarding computer security.

Texas Penal Code, Chapter 33: Computer Crimes

State of Texas law specifically pertaining to computer crimes. Among other requirements, unauthorized use of University computers or unauthorized access to stored data, or dissemination of passwords or other confidential information to gain access to the University's computer system or data is in violation of criminal law.

Texas Penal Code, Chapter 37: Tampering with Governmental Records

Any alteration, destruction, or false entry of data that impairs the validity, legibility or availability of any record maintained by the university is a violation of criminal law.

United States Penal Code, Title 18, Section 1030: Fraud and related activity in connection with computers

Federal law specifically pertaining to computer crimes. Among other requirements, prohibits unauthorized and fraudulent access.

Federal Copyright Law

Recognizes that all intellectual works are automatically covered by copyright. The owner of a copyright holds the exclusive right to reproduce and distribute the work.

<http://www.copyright.gov>

Computer Fraud and Abuse Act of 1986

Makes it a crime to access a computer to obtain restricted information without authorization; to alter, damage, or destroy information on a government computer; and to traffic in passwords or similar information used to gain unauthorized access to a government computer.

Electronic Communications Privacy Act of 1986

Prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal.

Computer Software Rental Amendments Act of 1990

Deals with the unauthorized rental, lease, or lending of copyrighted software.

Examples of Common Computing Violations

The table below will provide you with specific information you need to use the Tarleton computing resources responsibly.

Types of Violations

Abuse of Technology Resources:

Disruptive or mass mailings (mail bombing).

Disruptive print jobs.

Tying up workstations.

Adding a hub to the existing network.

Installing a web server or other server to provide applications, software, or files (e.g., BBS, Chat, DHCP, DNS, FTP, IRC, NTP, NNTP, POP2/3, SMTP, or WINS) on your microcomputer

Destroying or altering data or programs belonging to others (virus planting).

Improper Use of Accounts:

Chain letters and "Make Money Fast" schemes.

Message to all faculty and staff for non-business use; i.e., giving away free kittens or selling a sofa.

Commercial use of resources for personal gain.

Permitting another individual to use your account.

Using someone else's account.

Misappropriation of Intellectual Property:

Owning unlicensed copies of copyrighted materials (software & MP3 piracy).

Distribution of unlicensed copies of copyrighted material (software, MP3, etc.).

Invasion of Privacy:

Password cracking.

Network sniffing.

Unauthorized access to files and programs.

Harassment:

Using electronic communications to create a hostile work or learning environment.

Impersonating other individuals electronically.

Restricting access/denial of service.

Disclaimer: Other policies, regulations, rules, procedures, and laws may exist which cover these and other areas of technology use. It is not the intention of this list to be the only source of such information. Current TAMUS and Tarleton rules, regulations, and policies will control any infraction regardless of what may appear on these pages.

University Maintained Distribution Lists

The University provides and maintains these distribution lists:

Students	all students
Faculty	all faculty
Staff	all staff
k_students	Killeen students
k_faculty	Killeen faculty
k_staff	Killeen staff
s_students	Stephenville students
s_faculty	Stephenville faculty
s_staff	Stephenville staff

These lists allow the university to distribute information quickly but consume university resources and time. It is important to use these lists prudently and for university-related information only.

Please do not use the faculty, staff and students lists for:

Personal messages

Chain or mass-forwarded messages

Commercial messages, particularly item for sale or give-away

Large graphic files

Anything unrelated to the business of the university

University Approved Channels for Personal Communication

A bulletin board is available at <http://www.tarleton.edu/main/bb/> for personal communication and non-business related messages.

There is a list serve, l_students, for open communication among students. Students may subscribe and unsubscribe to this list as desired.

To subscribe, send a mail message to mailserv@tarleton.edu:

Subject can be anything.

Text of the message: subscribe l_students username@tarleton.edu

To unsubscribe, send a mail message to <mailto:mailserv@tarleton.edu>

Subject can be anything.

Text of the message: unsubscribe l_students username@tarleton.edu

You should receive confirmation of your request. Please contact the Help Desk at 968-9885 if you need further assistance.

Please remember that any commercial use of state resources is against both Tarleton rules and The Texas A & M University System regulations.

OFFICE OF RESPONSIBILITY: Information Resources