Department of Student Activities
Student Government Association
Computing Use, Ethics, and Information Confidentiality

Hardware

The Student Government Association (SGA) provides committees, commissions, and other student leaders with a workstation, server space, and for some an email account. SGA also maintains printers, phones, walkie-talkies, and a camera that can be assigned to individuals. This equipment is to be used for the SGA operations and functions consistent with the mission and values of the organization. These operations include administrative functions, customer service activities, program marketing and management, and student development opportunities.

Student leaders within SGA should be familiar with Texas A&M University rules regarding the proper use of university computers and network access. It is the responsibility of all student leaders to read and understand the following sections of the University rules:

http://rules.tamu.edu/urules/300/330499m2.htm (Rule 33.04.99.M2) Rules for Responsible Computing

http://rules.tamu.edu/urules/300/330499m3.htm (Rule 33.04.99.M3) Incidental Computer Use

http://student-rules.tamu.edu/rule22.htm (Rule 22.1-22.2) Student Rule for Responsible Computing

Software

The DSA-AD Information Technology team has a list of approved application to be loaded on all Desktops. Specialized applications may require approval from a Supervisor or Director prior to installation. New packages must be tested within the DSA-AD test network before being deployed, and proper licensing for each must be maintained in the IT office for the appropriate department.

Default User Desktops

- Pre-Approved applications
    - NAV – Anti-Virus Corporate Edition
    - MS office 2000/XP/2003, MS Publisher, Access, FilemakerPro
    - Hummingird/3270 Emulation Software/Entire Connection
    - WinZip with appropriate License
    - IE 5.5 SP2/6.0
    - Adobe Creative Suite
    - No shareware – Special applications required for specific job duties should be approved by Supervisor

Software license and copyright conditions:

- SGA Student Leaders must be aware of and comply with software license and copyright conditions.
- Texas A&M University licenses software from a variety of companies. In general, the university does not own this software or related documentation and, unless authorized by the software owner, does not have reproduction rights.

- Texas A&M University purchases software, or the right to use software, from a variety of companies. The copyrights for the software and documentation must be respected.

- With regard to use on local area networks or on multiple machines, Student Leaders shall use the software only in accordance with the license agreement.

- Student Leaders shall not be party to unauthorized use or copying software.

- Personal Software – if installing software that is not licensed by the department, a copy of the license must be submitted to the technology services area. If the software is not on the approved list, written approval from your supervisor must also be submitted.

Passwords

DSA Account Policy Settings & Password Policy

- Enforce password history – 3 passwords remembered (the system remembers the last three passwords you have used, must have a unique password, cannot use the repeat the same three.)

- Maximum password age – 90 days

- Minimum password age – 1 day

- Minimum password length – 8 characters

- Passwords must meet complexity requirements – yes

- Store password using reversible encrypt – no

- Account Lockout Policy

- Account lockout duration – 10 minutes

- Account lockout threshold – 3 invalid logon attempts

- Reset account lockout counter after - 10 minutes

- All Passwords must be of 8 - 14 characters in length with at least one special character. Characters at the beginning of your password make it harder to decipher and are required. Example: %, or &

- Passwords Complexity required - Passwords should contain at least one upper-case Alphabetic character (A-Z), at least one lower-case Alphabetic character (a-z), and at least one Numerical character (0-9).

- Passwords should not be constructed from common English words, personal names, nicknames, names of family members or pets, favorite colors, birth-dates, phone numbers, home addresses, initials of family/spouse, credit-card numbers, or any other significant or personally-meaningful item which could be guessed by someone who knows you well. Example: Create a password from a phrase, i.e. %1m&Aggie

- Passwords should not be constructed of simple progressive characters. ('abcdefg...' or '12345...')

- Use of some Symbol Characters is highly recommended, i.e. ~!#$%. The use of Control Characters is NOT recommended.

- Passwords should not be written on the desk or monitor, or in an easily accessible location such as a desk-drawer, address book, or other such item.

- Passwords should not be given out to allow another user access to your files. Contact your Network Administrator and the user can be given access to the files you specify without compromising your password.

- Do not share your login with another user, or leave your machine unlocked while you are away from it - even for a brief time.

- Password changes will be required every 90 days.

- Account Lock Out after the 3rd attempt

- Password History maintained - 3

Information Confidentiality

- Confidentiality of student information will be maintained (this includes grades, student ID, and student address information)

- Programs, files, E-mail, or data belonging to others will not be accessed, altered, or copied without prior authorization from the owner. In general, this authorization must be in writing. Routine maintenance is exempted from this requirement. In most cases where system integrity is an issue, immediate intervention may be taken. Such intervention is to be limited in its scope and is to be reported to the primary advisor to the Student Government Association

- In those cases where University Police, other police, or other appropriate agencies request access in conjunction with an investigation, the request should be in writing and reported to the Information Security Function (at CIS) as well as the appropriate Department of Student Activities director as soon as practical.

- The following statement will be use as a signature for email:

  This e-mail and any files transmitted with it are confidential. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or use of the contents of this information is prohibited. If you have received this e-mail transmission in error, please notify me by telephone or via return e-mail and delete this e-mail from your system.

Expectations for Shared Computers:

All students are required to LOG OUT of their work station prior to leaving it. If the student does not log out, this locks the workstation and prevents the next user from effectively logging in. In the event a work station becomes locked, the computer will be reset and any data that is not saved will be lost.

User File Backup Information

All information that an individual wishes to have backed up daily needs to be placed into their "My Documents" folder. Any information saved to the desktop will not be backed up and the Computing Operations staff will not be responsible for the loss of information not stored in the proper location.

Privacy

Computing equipment issued to students and electronic information stored on workstations and servers are the property of Texas A&M University. Review of student files and confiscation of computing resources is permitted when a business necessity for doing so has been established by the primary advisor to the Student Government Association.

As a precaution, personal files should be maintained on personal computers owned by students.

Email and Calendar
Student email accounts are issued to facilitate and improve SGA communication. All student email activity should comply with the expectations set forth in the Texas A&M University rules related to email use (University Rule 33.04.99.M2) (Link – Once Activated)

To facilitate scheduling, Microsoft Outlook Calendars can be viewed by all staff members within the Department of Student Activities. All students are encouraged to utilize MS Outlook to record business related appointments and other commitments during the workday.

Violations
Students involved in the **Student Government Association** are cautioned that any violation of the computer ethics standards contained in this document may be grounds for disciplinary action. Depending on the seriousness of the violation such actions may affect a student's *good standing status* within the university, financial restitution for unauthorized use of services, and misdemeanor or felony charges in a court of law.

Students are expected to conduct themselves in accordance with the regulations and responsibilities as published in the Texas A&M University Rules. Further, students are expected to conduct themselves in accordance with the Texas A&M University Student Rules.

I have read and understand the standards of conduct expected of me as an employee of Texas A&M University.

_____ _____

Name Date

33.04.99.M2 - Rules for Responsible Computing

Approved August 27, 1997

Supplements System Policy 33.04 and the TAMUS Ethics Policy 07.01

1. GENERAL

1.1 Texas A&M University recognizes the importance of the 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 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, 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, Texas A&M University's philosophy about computing use. Additional information can be found in Texas A&M University System Policies and Regulations, Texas A&M University Rules (formerly Texas A&M University Policies and Procedures Manual), and the Texas A&M University Student Rules (formerly University Regulations).

2. FREEDOM OF EXPRESSION

Censorship is not compatible with the goals of 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, 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 work stations, 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. Others are not permitted to use accounts or passwords. 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 as defined in TAMU Computer Security Rules 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 about computing from the system operator.

7.1.7 Report any incidents of harassment using University computing resources and facilities according to guidelines in University Rule 34.01.99.M1. It may be harassment if

4. the behavior is unwelcome; and
5. the behavior interferes with your ability, or the ability of others to work or study; and
6. 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.

"Texas A&M University is committed to providing an educational and work climate that is conducive to the personal and professional development of each individual. To fulfill its multiple missions as an institute of higher learning, Texas A&M University encourages a

climate that values and nurtures collegiality, diversity, pluralism and the uniqueness of the individual within our state, nation, and world. The University also strives to protect the rights and privileges and to enhance the self-esteem of all its members. Faculty, staff, and students should be aware that any form of harassment and any form of illegal discrimination against any individual is inconsistent with the values and ideals of the University community." (University Statement on Harassment and Discrimination, University Student Rules, p.3.)

Office of Responsibility:
Associate Provost for Information Technology

33.04.99.M3 - Incidental Computer Use

Approved September 16, 1996
Revised September 17, 1997
Revised November 11, 1999
Supplements System Policy 33.04

1. **GENERAL**

   Incidental personal use of computing resources at Texas A&M University is an exception to the general prohibition against the use of University equipment for anything other than official state business.

2. **GUIDELINES**

2.1 Incidental personal use of computing resources facilitates the user's proficiency. Incidental Computer Use is defined as:

2.1.1 occasional use for personal purposes,

2.1.2 of minimal time and duration, and

2.1.3 that results in no additional cost to the University

Incidental Computer use must not interfere with assigned job responsibilities or be in violation of existing security/access rules.

2.2 Except for incidental personal use connected with approved outside employment/consulting, incidental personal use must not:

2.2.1 result in financial gain for the user,

2.2.2 be for business purposes where the business is owned by the employee or the work is done for another business.

3. Personal use of University computing resources for consulting or outside employment, or which cannot be categorized as incidental should be guided by System Regulation 33.04.01: Use of System Resources for Outside Professional Activities.

OFFICE OF RESPONSIBILITY:
Vice President and Chief Financial Officer

33.04.01 Use of System Resources for External Employment

April 24, 1996, Revised July 18, 2001

Supplements System Policy 33.04

---

1. COMPETITION WITH THE PRIVATE SECTOR

System resources may not be used to compete unfairly with private sector entities or private consultants.

2. EXTERNAL EMPLOYMENT

External employment includes consulting or other professional employment activities for which a faculty or staff member is compensated by a third party. System resources and services may not be used by the faculty or staff member unless the external employment has been approved by the component.

3. INCIDENTAL USE OF SYSTEM RESOURCES

Faculty or staff members may occasionally use their offices, library resources, office telephones for local calls, office equipment (including personal computer) and other resources for approved external employment (See System Regulation 31.05.01) if the use of these resources does not cause an additional expense to the System or an illegal conversion of System resources to private use.

4. SIGNIFICANT USE OF SYSTEM RESOURCES

4.1 Significant Use of Resources Subject to Charge

4.1.1 A faculty or staff member in the course of performing approved external employment may not charge long distance telephone calls to a System account, use System personnel to perform services of any type, perform computing on a mainframe or departmental minicomputer facility, make use of a departmental copier, or otherwise use resources of the System related to the external employment, without paying for such services on a fee or contract basis that allows the System to recover its costs.
4.1.2 Arrangements for the use of and reimbursement for such resources and services must be in writing and approved in advance. The Chancellor's authority to approve such arrangements, set forth in System Policy 33.04, Use of System Property, is hereby delegated to Chief Executive Officers (CEOs), or designee(s).
4.2 Services Available to the General Public
System services regularly available to private individuals or firms on a fee or per-unit basis may be secured by System employees at the same cost and under the same conditions that they are available to the general public.
4.3 Contracting for Use of System Resources
A faculty or staff member engaged in approved external employment may contract with the System for personnel services, laboratory services, supplies, computing services, equipment use, and similar resources. Such contracts must be approved in advance using established contracting guidelines, including provisions for the payment of the components' indirect costs. Contracts for the use of System resources must be approved in advance by the CEO, or designee. Approval may be given only when all of the following conditions are met:
(1) the requested resources are not reasonably available from the private sector, even at a somewhat higher cost;
(2) the contract provides for the payment to the component of indirect costs;
(3) the proposed work contributes to the advancement of System programs and/or to the professional development of personnel;
(4) the use of resources for this activity will not interfere with or detract from the regular educational, research or service activities of the System; and
(5) no conflict of interest exists between the proposed work and existing or anticipated activities of the individuals concerned or the System. (Caution should be exercised in hiring graduate students to assist in consulting.)

5. MONITORING

CEOs of System components must monitor all use of System resources under this regulation.

22. Rules for Responsible Computing (Revised: 1996)

22.1 Use of university computing 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 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 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 rules and/or laws.

22.2 As an institution of higher learning, 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, Texas A&M University's philosophy about computing use.

22.2.1 Freedom of Expression: Censorship is not compatible with the goals of Texas A&M University. The university should not limit access to any information due to its content when it meets the standard of legality.

22.2.2 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 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.

22.2.3 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. Unless permission of the author is obtained, utilization of any electronically transmitted information must comply with the "fair use" principle.

22.2.4 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 racial, ethnic, religious or sexual harassment.

22.2.5 Authorized Use: Computing resources are provided by the university to accomplish tasks related to the university's mission. Some computers may be dedicated to specific research or teaching missions that limit their use. Computing resources may not be used for unauthorized commercial activities or any illegal activities. Incidental personal use of computing resources by employees is governed by The Texas A&M University System Ethics Policy. (see Appendix V)