

INFORMATION RESOURCES ACCEPTABLE USE POLICY

The University of Texas at San Antonio (UTSA) relies on networked computers and the data contained within those systems (Data) to achieve its missions. This Acceptable Use Policy is to protect these resources in accordance with state law and U. T. System Regents' Rules and ensure that UTSA can access Data to fulfill its duties and mission. All individuals granted access to UTSA Information Resources must be familiar with and follow the acceptable use rules below:

General

- UTSA information resources are provided for the express purpose of conducting the business and mission of the University.
- UTSA information resources must not be used to: engage in acts against the mission and purposes of the University, intimidate or harass, degrade performance, deprive access to a University resource, obtain extra resources beyond those allocated, or to circumvent computer security measures.
- Information resources must not be used to conduct a personal business or used for the exclusive benefit of individuals or organizations that are not part of The University of Texas System
- Sexually Explicit materials must not be intentionally accessed, created, stored or transmitted other than in the course of academic research where this aspect of the research has the explicit written approval of an Executive Officer of UTSA
- Faculty, staff, students, contractors, guests, or others users (Collectively "Users") must not copy or reproduce any licensed software except as expressly permitted by the software license, use unauthorized copies on University-owned computers or use software known to cause problems on University-owned computers.

Information Services Privacy

- Users, have no expectation of privacy regarding any Data residing on UTSA computers, servers, or other information resources owned or held on behalf of UTSA regardless of whether the Data was generated as the result of acceptable (including Incidental Use as described below) or unacceptable use of UTSA's information resources.
- All files, documents, messages in any format and other Data residing on UTSA computing resources or held on behalf of UTSA are owned by the institution in accordance with the Regents' Rules and Regulations and are subject to access by the institution without notice to comply with public information requests, court orders, subpoenas or litigation holds; or for any other purpose consistent with the duties of the institution. Users, including students, staff and faculty members, have no expectation of privacy in any such Data,

Data Protection

- Data will be accessed in order to comply with the duties of UTSA on a need to know basis. Users of UTSA information systems must not attempt to access data or programs contained on systems for which they do not have authorization or consent.
- All critical University data (electronic files) will be saved on network servers to ensure backup of the data. All data, including research data, should be backed up for disaster recovery reasons.
- All records (electronic or paper) will be maintained in accordance with the UTSA Records Retention Policy.

Virus Protection

All computers connecting to the UTSA network must run current and authorized virus prevention software. Virus protection software must not be disabled or bypassed except as required by the temporary installation of software or for other special circumstance. Computers found to be infected with a virus or

other malicious code will be disconnected from the UTSA network until deemed safe by The Office of Information Technology (OIT).

Electronic Mail

- The following electronic mail (email) activities are prohibited by policy:
 - Using email for purposes of political lobbying or campaigning except as permitted by the Regents' Rules and Regulations.
 - Posing as anyone other than oneself when sending email, except when authorized to do so by the owner of the email account.
 - Reading another user's email unless authorized to do so by the owner of the email account, or as authorized by policy for investigation, or as necessary to maintain services.
 - Use of email software that poses a significant security risk to other Users on the UTSA network.
 - Sending or forwarding "chain" letters.
 - Sending unsolicited messages to large groups except as required to conduct University business.
 - Sending excessively large messages or attachments unless in performance of official University business.
 - Sending or forwarding email that is likely to contain computer viruses.
- Delivery of electronic mail is not guaranteed.

Confidential or Protected Information

- Users shall not disclose confidential information except to authorized parties as required to accomplish authorized business functions in support of the institutional missions.
- All confidential or protected health or student information transmitted over external networks or saved on University servers must be encrypted in accordance with OIT Encryption Guidelines. This information must not be sent or forwarded through non-University email accounts provided by other Internet Service Providers, and must not be knowingly transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols and security techniques are utilized.

Incidental Use of Information Resources

- Incidental personal use of electronic mail, internet access and other information resources by an employee is permitted by University policy but is restricted to employees (it does not extend to family members or other acquaintances). It must not interfere with normal performance of an employee's duties, must not result in direct costs to UTSA and must not expose the University to unnecessary risks.
- Storage of any non-work related email messages; voice messages, files and documents within the UTSA email system must be nominal (less than 5% of a User's allocated mailbox space).
- Non-work related information may not be stored on network file servers.

Internet Use

- Software for browsing the Internet is provided to authorized Users for business, education, research, and patient care purposes.
- Due to network maintenance and performance monitoring and to ensure compliance with applicable laws and policies, all user activity may be subject to logging and review.
- Email or postings by Users of UTSA network resources to news groups, "chat rooms" or "listservs" must not give the impression that they are representing, giving opinions, or making statements on behalf of UTSA, unless authorized. Users should use a disclaimer stating that the opinions expressed are their own and not necessarily those of UTSA.

- Personal commercial advertising must not be posted on UTSA web sites.

Portable and Remote Computing

- All computers and portable-computing devices using UTSA information resources must be password protected using the “strong” password standard adopted by UTSA to prevent access by unauthorized parties. At a minimum, such passwords are to be changed in accordance with the University’s Password Guidelines, or immediately if there is suspicion that the password has been compromised.
- Employees accessing the UTSA network from a remote computer must adhere to all policies that apply to access from within the local campus network. Remote computers are subject to the same rules and security related requirements that apply to University-owned computers.
- Unattended portable computing devices must be physically secure.
- If it is determined that required security related software is not installed on a remote computer or that a remote computer has a virus, is party to a cyber attack or in some way endangers the security of the UTSA, the account and/or network connection will be disabled. Access will be re-established once the computer or device is determined to be safe by OIT.
- Users must not divulge UTSA, dialup or modem phone numbers to anyone.
- If critical data is stored on portable computing devices it must be backed up to a network server for recovery in the event of a disaster or loss of information.
- Special care should be taken to protect information stored on laptops and PDA devices, and in protecting such devices from theft.

Decentralized Technical Resources

- To provide specialized capabilities and services quickly and conveniently, some technical resources at UTSA may be operated and maintained by individual colleges or departments.
- Decentralized technical resources may be connected to the University network if they are administered by qualified technical staff and if they adhere to established policies.
- Faculty, students or staff who are designated administrators of decentralized technical resources are responsible for maintaining the appropriate security environment on their systems, including current virus scanning software and operating system security updates.
- To protect UTSA data and technical resources, decentralized computers or servers will be disconnected from the University network if a threat is posed from that system by a virus, cyber attack or other means. The offending system may be reconnected once it has been restored to a safe condition.

Passwords

- In order to preserve the security of UTSA information resources and Data, every UTSA computer/network account, password, any personal identification number (PIN), digital certificate, security token (i.e. Smartcard), or any other similar information or device used for identification and authorization purposes must not be shared. Each user of UTSA resources is responsible for all activities conducted using his or her account(s).
- Digital certificate passwords used for digital signatures must never be divulged to anyone.
- Users must not circumvent password entry through use of auto logon, application “remember password” features, embedded scripts or hard-coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the Information Security Officer (ISO). Any exception situation must include a procedure to change the passwords and must adhere to security policies for password construction. (For more information, see the University’s Password Guidelines.)

Security

- Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems should not be downloaded and/or used, except as authorized by OIT. For example, password cracking programs, packet sniffers, or port scanners on University information resources shall not be used. Users must report any identified weaknesses in UTSA computer security and any incidents of possible misuse or violation of this agreement to an immediate supervisor, department head, or OIT.
- Where technically feasible, all PC's, laptops, personal digital appliance (PDA) devices and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less to prevent unauthorized access to the device.

Last Revised: October 14, 2011

Effective Date: October 15, 2011

Compliance Date November 30, 2011