The University of Texas At Tyler INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

The University of Texas at Tyler relies heavily on networked computers and the data contained within those systems to achieve its missions. This Acceptable Use Policy is to protect these resources in accordance with state law and Regents Rules. All individuals granted access to U. T. Tyler Information Technology are governed by state law and Regents Rules, specifically UTS 165, UT System Information Resources Use and Security Policy and must follow the acceptable use rules below:

General	•U. T. Tyler Information Technology is provided for the express purpose of conducting the business of U. T. Tyler. (UTS 165) •U. T. Tyler Information Technology must not be used to: engage in acts against the mission and purposes of U. T. Tyler, intimidate or harass, degrade performance, deprive access to a U. T. Tyler resource, obtain extra resources beyond those allocated, or to circumvent U. T. Tyler computer security measures. •Information Technology 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. Any exceptions must be in support of System missions and require the prior written approval of an executive officer. •Pornographic 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. •Email or postings by employees to news groups, chat rooms or listservs must not give the impression that they are representing, giving opinions, or making statements on behalf of U. T. Tyler unless authorized (explicitly or implicitly) to do so. Employees should use a disclaimer stating that the opinions expressed are their own and not necessarily those of U. T. Tyler, unless the posting is related to normal business responsibilities or unless it is clear from the context that the author is not representing U. T. Tyler. An example of a simple disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer." (UT Tyler Email Policy) •Staff must not copy or reproduce any licensed software except as expressly permitted by the software license, must not use unauthorized copies on University-owned computers or must not use software known to cause problems on UT Tyler computers. (COPYRIGHT LAW)
Data Protection	•Data will be accessed on a need to know basis. Users of Information Technology must not attempt to access data or programs contained on systems for which they do not have authorization or explicit consent. •All University data (electronic files) will be saved on network servers, whenever possible, to ensure backup of the data. When network storage is unavailable, all files containing University data must be password protected to prevent unauthorized access. •All records (electronic or paper) will be maintained in accordance with the U. T. Tyler Records Retention Policy.
Virus Protection & Security Patches	•All computers connecting to the U. T. Tyler network must run current virus prevention software. This software must not be disabled or bypassed with the exception of installation of software, or other special circumstance or procedure that requires the temporary disabling of virus prevention software. Computers found to be infected with a virus or other malicious code will be disconnected from the U. T. Tyler network until deemed safe by the Office of Information Technology and Communications (OISC). . (UT Tyler Network Policy) •All computers connecting to the U. T. Tyler network must be current on operating system and application critical updates and security patches. Computers found to be deficient in security patches will be disconnected from the U. T. Tyler network until deemed safe by the Office of Information Systems and Communications (OISC). (UT Tyler Network Policy)
Email	•The following email activities are prohibited by policy: -Using email for purposes of political lobbying or campaigning except as permitted by the Regents' Rules and Regulations. (UT Tyler Email Policy) -Posing as anyone other than oneself when sending email, except when authorized to do so by the owner of the email account. (UT Tyler Email Policy) -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. (UT Tyler Email Policy) -Use of email software that poses high security risks to U. T. Tyler Information Technology. -Sending or forwarding chain letters. (UT Tyler Email Policy) -Sending unsolicited messages to large groups except as required in conducting U. T. Tyler business. (UT Tyler Email Policy) -Sending excessively large messages or attachments unless in performance of official U. T. Tyler business. (UT Tyler Email Policy) -Sending or forwarding email that is likely to contain computer viruses. (UT Tyler Email Policy)
Confidential or Protected Information	•All confidential data and/or protected health information must not be sent or forwarded through non-U. T. Tyler email accounts (i.e. Hotmail, Yahoo, AOL, or email 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. •All confidential data and/or protected health information must not be transmitted via unencrypted instant messaging programs such as AOL Instant Messenger, MSN Messenger, Yahoo, or ICQ. (SRRPUB04)

Incidental Use of Information Technology	•Incidental personal use is permitted by the Information Technology Use and Security Policy but is restricted to U. T. Tyler 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 U. T. Tyler, and must not expose the University to unnecessary risks. (UTS 165) •Storage of any non-work related email messages including any attachments within the U. T. Tyler email system must be nominal (less than 5% of a User's allocated mailbox space). (UT Tyler Email Policy) •Non-work related files may not be stored on network file servers. (UTS 165)

	•All messages, files and documents stored on U. T. Tyler computing resources - including personal messages, files and documents - are owned in accordance with the Regents' Rules and Regulations. (UT Tyler Email Policy and UTS 165) •Any files, messages or documents residing on U. T. Tyler computers may be subject to public information requests and may be accessed in accordance with this policy. (UT Tyler Email Policy) •A University of Texas at Tyler email account should not be used for personal email correspondence confidential in nature. •Delivery of email not related to University business is not guaranteed.
Internet Use	•Software for browsing the Internet is provided to authorized users for business and research 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. •Personal commercial advertising must not be posted on U. T. Tyler web sites.
Network Device Connection	•All devices which are connected to the U. T. Tyler local area network (LAN), either via a hard-wire cable connection or a wireless connection, must be reported to the Office of Information Systems and Communications (OISC) for approval. (UT Tyler Network Policy) •For more information on devices connecting to the U. T. Tyler network, please view the U. T. Tyler Network Connection Policy at http://www.uttyler.edu/inforesources/uttnetworkpolicy.pdf (UT Tyler Network Policy)
Portable and Remote Computing	•All computers and portable-computing devices using U. T. Tyler Information Technology must be password protected using the "strong" password standard to be changed at least annually or if there is suspicion that the password has been compromised. •Employees accessing the U. T. Tyler network from a remote computer must adhere to all policies that apply to use from within U. T. Tyler facilities, must conform to the OISC minimum standards for portable computing, and 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 U. T. Tyler network, 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 OISC. •If critical U. T. Tyler data is stored on portable computing devices it must be backed up to a network server, whenever possible, for recovery in the event of a disaster or loss of information. When network storage is unavailable, all files containing University data must be password protected to prevent unauthorized access. •Special care should be taken to protect information stored on laptops and PDA devices, and in protecting such devices from theft.
Passwords	•U. T. Tyler account(s), passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes must not be shared (including with family members). Each User is responsible for all activities conducted using his or her account(s). (UTS 165) •Digital certificate passwords used for digital signatures must never be divulged to anyone. (UTS 165) •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 U. T. Tyler 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 OISC 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 the OISC. For example, password cracking programs, packet sniffers, or port scanners on U. T. Tyler Information Technology shall not be used. Users must report any identified weaknesses in U. T. Tyler computer security and any incidents of possible misuse or violation of this agreement to an immediate supervisor, department head, or the U. T. Tyler ISO. (Section 33.02 Texas Penal Code) •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.

User Acknowledgment I acknowledge that I have received and read the Information Technology Acceptable Use Policy. I understand that I must comply with the Policy when accessing and using Information Technology and my failure to comply with the Policy may result in appropriate disciplinary action and/or action by law enforcement authorities.
Signature: _____ Date_____ Print Name:_____