SUB-TOPIC

Information Resources Acceptable Use Policy

The University of Texas at Dallas ("UTD") relies heavily on networked computers and the data contained within those systems to achieve its missions. The Acceptable Use Policy is to protect these resources in accordance with state law and The University of Texas System Board of Regents' Rules and Regulations. All individuals granted access to UTD Information Resources must follow the acceptable use rules below:

General	• UTD Information Resources are provided for the express purpose of conducting the business of The University of Texas at Dallas. • Information Resources must not be used to: engage in acts against the missions and purposes of UTD, intimidate or harass, degrade performance, deprive access to a UTD resource, obtain extra resources beyond those allocated or to circumvent UTD 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 UTD. Any exceptions must be in support of The University mission and require the prior written approval of an executive officer. • UTD users must adhere to the U. T. System policy with regard to obscenity. • E-mail or postings to news groups, chat rooms or listservs must not give the impression that they are representing, giving opinions or making statements on behalf of UTD unless authorized (explicitly or implicitly) to do so. Individuals should use a disclaimer stating that the opinions expressed are their own and not necessarily those of UTD, unless the posting is related to normal business responsibilities or it is clear from the context that the author is not representing UTD. An example of a simple disclaimer is: "The opinions expressed are my own and not necessarily those of UTD." • Staff, faculty and students must not copy or reproduce any licensed software except as expressly permitted by the software license, use unauthorized copies of software or software known to cause problems on UTD owned computers.
Data Protection	• Data will be accessed on a need to know basis. Users of information systems must not attempt to access data or programs contained on systems for which they do not have authorization or explicit consent. • All mission critical UTD data (electronic files) will be saved on network servers to ensure backup of the data. • All records (electronic or paper) will be maintained in accordance with the UTD Records Retention Policy.
Virus Protection	• All computers connecting to the UTD 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 UTD network until deemed safe by the UTD Information Security Office.
E-mail	• The following E-mail activities are examples of activities prohibited by The University of Texas at Dallas E-mail Policy: - Using E-mail for purposes of political lobbying or campaigning except as permitted by The University of Texas System Regents' Rules and Regulations. - Use of web E-mail accounts is not allowed unless the provider scans mail for viruses, ex. Hotmail. - Sending or forwarding chain letters outside UTD. - Sending messages in violation of the CAN Spam Act, 15 USC 7701. - Sending large messages or attachments unless in performance of official UTD business. - Falsifying E-mail headers or newsgroup postings.
Confidential or Protected Information	• All confidential or protected health information transmitted over external networks must be encrypted. This information must not be sent or forwarded through non-UTD E-mail accounts (like Hotmail, Yahoo, AOL, or E-mail 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. Digital Certificates are provided for encrypting confidential information in E-mail. If instant messaging is used, it must be encrypted and UTD approved.
Incidental Use of Information Resources	• Incidental personal use is permitted by The University of Texas at Dallas Information Resources Use and Security Policy but is restricted to UTD authorized users; (it does not extend to family members or other acquaintances). It must not interfere with performance of normal duties or activities, must not result in direct costs to UTD, and must not expose UTD to unnecessary risks. • Storage of any non-work related E-mail messages; voice messages, files and documents within the UTD E-mail system must be nominal (less than 5% of a User's allocated mailbox space). • Non-work related files may not be stored on network file servers. • All messages, files and documents stored on UTD computing resources - including personal messages, files and documents - are owned in accordance with The University of Texas System Regents' Rules and Regulations. • Any files, messages or documents residing on UTD computers may be subject to public information requests and may be accessed in accordance with this policy. • A UTD E-mail account should not be used for personal E-mail correspondence confidential in nature.

Internet Use	• 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 UTD web sites.
Portable and Remote Computing	• All computers and portable-computing devices using UTD Information Resources must be password protected using the "strong password" standard and be changed at least semi-annually or more frequently if there is suspicion that the password has been compromised. • All users accessing the UTD network either remotely or locally from personal or UTD-owned computers must adhere to all policies that apply to use from within UTD facilities and are subject to the same rules and security related requirements that apply to UTD-owned locally-connected 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 UTD 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 the UTD Information Security Office. • If critical UTD 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.
Passwords	• UTD 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 or acquaintances). Each user 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 to UTD systems 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 UTD 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 UTD 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 Information Security Office. For example, password cracking programs, packet sniffers, or port scanners on UTD Information Resources shall not be used. Users must report any identified weaknesses in UTD computer security and any incidents of possible misuse or violation of this agreement to an immediate supervisor, department head, the Executive Director of Information Resources or the UTD Information Security Officer. • Where technically feasible, all PC's, laptops, personal digital appliance (PDA) devices and workstations in public areas 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. When located in an attended or locked office, a password-protected screen saver setting of 60 minutes is sufficient.

User Acknowledgment

I acknowledge that I have received and read The University of Texas at Dallas Information Resources Acceptable Use Policy. I understand that I must comply with the policy when accessing and using Information Resources 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:_____