Message from the CIO

It's that time of year again – TTU is “Back to School!” In this issue we provide **Safe Computing Reminders**, so you can start your new semester off with safe computing practices. The IT Division, Office of the CIO, welcomes TTU students, faculty, and staff as well as those students joining us in the wake of the Hurricane Katrina disaster. We extend our warmest welcome and are here to support you in having a productive semester. As always we encourage you to “Practice Safe Computing.”

- Sam Segran
  Associate Vice President for IT and Chief Information Officer

---

**eRaider Password Expiration Policy and Guidelines**

At Texas Tech University, your eRaider Account is your electronic identification. Your eRaider account allows you access to a variety of campus resources. Based on auditor recommendations and a heightened institutional awareness of security practices, the IT Division strongly advises:

- Do not share your password with anyone else
- Do not re-use your eRaider password for other purposes
- Do not write down your eRaider password, if you do, keep it in a safe place; develop a system for remembering your password
- Never leave your computer system unattended when you are logged in with your eRaider account
- If you have to leave your system unattended, lock the computer

**Passwords must:**

- 8-15 alphanumeric characters
- Include at least one lower case character
- Include one upper case character
- Include one number (numeric character must not be at the beginning or the end of the password)
- Not contain common words and abbreviations found in a dictionary

**Avoid the following as a password:**

- Username
- Employee number
- Name or family member names (including nicknames)
- Social Security Number
- Birthday
- Makes or models of vehicles
- License plate number
- Pet’s name
- Address
- Phone number
- Town, City, or State
- Reverse of any of the above

Please note that eRaider passwords must be renewed every ninety (90) days. You will receive three email notifications before password expiration (messages will cease once you change your password). In addition, you will be reminded each time you authenticate to an application.

Strong passwords may be a bit less convenient, but the practice guards against data theft and privacy violations. To view all IT Security Policies, please visit [http://www.infotech.ttu.edu/security/](http://www.infotech.ttu.edu/security/). If you have any questions, or for additional information, please contact IT Help Central at 742-HELP (4357).

**General Safe Computing Practices**

As faculty, staff, and students prepare for another busy fall semester, the IT Division has created a series of “Back to School” IT reminders. We recommend the following general safe computing practices:

**DO:**

- Install Symantec AntiVirus on your computer ([free download available at http://eraider.ttu.edu](http://eraider.ttu.edu))
- Turn on automatic Windows update feature ([http://windowsupdate.microsoft.com](http://windowsupdate.microsoft.com))
- Turn on the SPAM filter feature on your Outlook 2003, if you are using the University's TechMail Server for your email. More information at [www.helpdesk.ttu.edu/general/O2K3JunkEmail.php](http://www.helpdesk.ttu.edu/general/O2K3JunkEmail.php)
- Upgrade to the latest version of your software packages. ([Microsoft software is available for free download at http://eraider.ttu.edu](http://eraider.ttu.edu))
- Verify email attachments and links are valid before clicking
- Lock your computer system when you leave your office/study area/residence hall room with one of the following options:
  1. Use Control, Alt, and Delete keys then click on “Lock”
  2. Use the Windows Key + L
- Set your screensaver to activate password protection

**DO NOT:**

- Give out personal information (SSN, driver’s license number, credit card number, birth date, etc.) on web sites or in response to any email solicitation unless you have verified the authenticity of the business
- Open email attachments unless it is a file you are expecting
- Open suspicious emails
- Use peer-to-peer file sharing
- Forward chain letters and scams emails
- Click on links in unsolicited emails
- Send personal information (SSN, driver’s license, etc.) through email
- Leave your laptop or handheld device in a public area unattended

For additional assistance, please contact IT Help Central at 742-HELP (4357) or visit [http://safecomputing.ttu.edu](http://safecomputing.ttu.edu)

**Your Confidential Information**

Family Educational Rights and Privacy Act (FERPA) requires that each University community member be allowed to control the public release of their private information. “Public release” indicates anyone outside the University. You may elect to withhold personal information from publication in the Online Campus Directory.

**Specifically for students:**

- Go to TechSIS Web for Students [http://techsis.tomet.ttu.edu/student/](http://techsis.tomet.ttu.edu/student/)
- Log in with your eRaider username and password
- The “Student Services” page will be displayed. Under the heading “Personal Information” click on “Information Release Restriction”
- You may select information that you wish to withhold from publication (choose the box next to the information you wish to remain confidential)
- Click the “Update” button at the bottom of the page to submit your changes.
For faculty, staff, and students:
- Go to http://eraider.ttu.edu
- Log in with your eRaider username and password
- Click on "Manage your eRaider Account"
- On the left menu, click on "Online Directory Info"
- Choose "Yes" or "No" to be published in the Online Directory
- If you choose "Yes," then choose the information that will be listed online by checking the box
- Click "Save Changes" at the bottom of the page to update your information
- Be sure to log out of the eRaider Account Manager and close all windows.

Downloads and Copyright Restrictions
In 1998, an amendment was made to Title 17, which made major changes in U.S. copyright law to address the digitally networked environment. It is called the Digital Millennium Copyright Act (DMCA), and it represents a fundamental change in copyright law as applied to the Internet and digital works. Texas Tech strictly adheres to this law.

Particularly relevant DMCA highlights for TTU include:
- It is a crime to circumvent anti-piracy measures built into most commercial software.
- The manufacture, sale, or distribution of code-cracking devices used to copy software illegally is illegal.
- The cracking of copyright protection devices, in order to conduct encryption research, assess product interoperability, and test computer security systems is allowed.
- Exemptions from anti-circumvention provisions for nonprofit libraries, archives, and educational institutions are afforded under certain circumstances.
- States explicitly that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use...."
- Unauthorized duplication of copyrighted information or data and software packages is a direct infringement of the federal copyright law.

The TTU Information Technology Division avidly supports Texas Tech’s policies and the federal statutes regarding copyright infringement. It is illegal to make, use, or pass along unauthorized copies of software, graphics, music or any other creative art or intellectual property for multimedia projects or any other use. This includes the copying of software programs, etc., required in a class. Anyone who engages in illegal copying shall be subject to disciplinary action under Texas Tech’s policies and, in addition, shall be subject to criminal prosecution under state and federal statutes.

It is a violation for anyone to upload or download full-length sound recordings or DVDs without permission of the copyright owners. Using peer-to-peer (P2P) applications such as KaZaA, Morpheus, Grokster, and eDonkey is illegal. The current generation of P2P file-sharing programs, which allow an Internet user to search through MP3 libraries of other users with no Web site involved (as was the case with Napster), is also illegal.

The Recording Industry Association of America (RIAA) is a private, non-profit corporation, whose member companies produce, manufacture, and distribute approximately 90% of all legitimately recorded music in the U.S. The RIAA proactively audits public downloading and has targeted institutes of higher education in the recent past. Illegally downloading copyrighted files (piracy, counterfeiting, or bootlegging) violates:
- Texas Tech University policies (30.22.4 and 30.22.5, which relate to guidelines for audiovisual materials and music use)
- Federal laws (Title 17, Section 101 and Title 18, Section 2319, which protects copyright owners from the unauthorized reproduction or distribution of sound recordings, as well as certain digital performances to the public, and Title 18, Section 2319A, which criminalizes the unauthorized recording, manufacture, distribution or trafficking in sound recordings and music videos of "live" musical performances the anti-bootleg statute)

The only legal way to reproduce and transmit a piece of recorded music by uploading or downloading is to get permission from the owners of these different copyrights, which is termed obtaining a “license” for the recording.

Safe Computing Tips for Online Purchasing
1. Only purchase from secure web sites
   - Web address must begin with http://
   - The padlock in the lower right corner of the browser window is locked
2. Purchase from reputable vendors; to evaluate a specific vendor, visit http://www.bbb.org/
3. Do not provide SSN, drivers license number, credit card numbers, birth date, or other confidential information that is not necessary and reasonable for the purchase
4. If you have to create an account in order to purchase, do not use your eRaider username or password
5. Print your confirmation page and put in a secure location

For additional Safe Computing Practices information, please visit http://safecomputing.ttu.edu

Contributions by: Katherine Austin Stalcup Ph.D., Lori Dudley, Joshua Harrison, Amy Boren, Tiffany Naylor, and Carlene Van Stone

Safe Computing Practices Committee: Katherine Austin Stalcup Ph.D., Shannon Cepica, J Stalcup, Scott Hall, Eric Burrell, Lori Dudley, Tony Castle, Darrell Bareman, and assistance from IT Division Directors and other staff