Message from the CIO

As the University is busily engaged in the budgeting process as well as year-end procurements, we want to introduce our PC – Cradle to Grave initiative. Motivated by information security and judicious management of technology resources, the initiative addresses the following issues:

- As a result of state equipment disposal laws and regulations, we want to ensure that confidential TTU information on hard drives does not leave the University for transfer to other state agencies, such as school districts or the prison system.
- When equipment is transferred from one TTU department to another TTU department, we want to ensure that confidential departmental information is not transferred and that proprietary software is removed, congruent with copyright regulations.
- Given that some TTU departments may surplus systems that are superior to systems located in other TTU areas, this initiative has components that will enable departments to trade systems directly, in compliance with existing TTU Operating Policies. This method also ensures that TTU surpluses the oldest technology thereby increasing the coefficient of utilization of newer systems in the university.
- From a support perspective, non-standard equipment is more difficult and costly to support. This initiative includes existing corporate partnerships that allow TTU to standardize equipment and software (some college specific), while also lowering the purchase price for standard system bundles.

From procurement to disposal, the IT Division has a variety of services for the University community that are highlighted in this bulletin. In this issue, we also address password guidelines and the importance of strong passwords. In order to further protect information resources, including your eRaider accounts, passwords will be changed every ninety (90) days, in line with recommended industry and State of Texas IT security best practices as well as audit recommendations. We will be sending out more information as the new password changes are rolled out over the next few months. Remember that safe computing practices are vital to the health of your system!

Sam Segran
Associate Vice President for IT and Chief Information Officer

---

PC - CRADLE TO GRAVE TIME LINE - LIFE OF YOUR PC

**Stage 1: Procurement**

http://www.depts.ttu.edu/helpcentral/recommend.php

Through a partnership with DELL Computer Corporation, the TTU Information Technology (IT) Division has configured hardware bundles for Texas Tech University. Desktop and laptop bundles were created with input from the Network Site Coordinators, representing the colleges and departments. We also provide recommended configurations for handheld devices (standard and advanced). In addition, the DELL site (linked from the web address listed above) lists projectors at reduced prices for Texas Tech University. Specialized hardware bundles were configured for students and faculty in the following colleges:

- College of Engineering
- School of Law
- College of Architecture
- Discussions with other colleges are in progress.

For departmental orders, we have compiled a set of departmental recommendations and created e-PO forms available through the link above.

Hardware and software for personal (home) use by Texas Tech University students, faculty, and staff is available at this web site. This web site also highlights the discounts available on bundled systems recommended by TTU and other product discounts as available.

**Stage 2: Software**

http://www.itts.ttu.edu/software/

The TTU IT Division negotiates and maintains several site license contracts, providing various software programs to the University community at no charge. The following software can be downloaded from the eRaider Web site (http://eraider.ttu.edu):

- Microsoft Windows upgrades
- Microsoft Office
- Microsoft Visual Studio
- Microsoft FrontPage
- Microsoft Virtual PC for Mac
- Norton AntiVirus

Software such as SPSS, SAS, AutoCAD, GIS, and Maple are also available (some at a nominal cost). In addition to the software listed above, specialized software is available for use in all ATLC computer labs (http://www.itts.ttu.edu/labs).

**Stage 3: Getting Help**

Information Technology Help Central (IT Help Central) is committed to providing a single point of contact for computing solutions for students, faculty, and staff at TTU. Key services consist of computer support via telephone, walk-in, and e-mail; hardware and software configurations and purchase recommendations; and virus alerts/instructions to obtain virus definitions. For desktop support, colleges and departments should contact their local computing support staff for assistance. Those who are currently supported by IT Help Central should contact desktop support at IT Help Central. For more information please contact IT Help Central at 742-HELP (4357).

**Stage 4: Training**

Technology Support offers ShortCourses that are instructor-led, non-credit, 2-hour sessions designed to help the University community improve their computer skills. Topics include introduction to computer systems, safe computing practices, the Internet, e-mail, programming skills, Web publishing, graphical software, and Microsoft Office applications. For additional information, please visit http://www.itts.ttu.edu/training/shortcourses/ or call 742-1650.

Technology Support also provides Computer-Based Training (CBT). Online learning modules are self-paced and interactive, with self assessment tools incorporated in each lesson. To access our collection of 340 courses, please visit http://cbt.ttu.edu.
The IT Division sponsors periodic roundtables and vendor-supplied information sessions designed to address key technology topics and to provide recommendations to the University community. Some of the topics covered are security related, such as secure desktop management, secure computing lab management, and secure server management (currently being developed). For additional information, please visit http://safecomputing.ttu.edu.

Stage 5: Disposal
In collaboration with Property Management (Operations Division), the IT Division has created “Raider PC Mart,” a voluntary online communication system to allow departments to trade computer equipment (http://www.raiderpcmart.ttu.edu).

We strongly recommend that each department clean the hard drive of any system before transferring it to another department. To aid in this task, the IT Division is providing “KillDisk.” KillDisk is a utility that will erase entire hard drives, hard drive partitions, and floppy drives. KillDisk erases ALL data, including the operating system and, optionally, any partition information.

The IT Division has also purchased a degausser that Property Management will use to demagnetize all hard drives leaving the University. This ensures protection of University data. In order to aid in this effort, the Operations Division and the Office of the CIO are providing funding for this additional service.

Password Security Policies
The Texas Tech University Password Policy is in place to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the Texas Tech University user authentication mechanisms. In accordance with OP 52.04 Information Technology Security, the Texas Tech University Password Policy applies equally to all individuals who use or administer any Texas Tech University computing system or information resource. Access gained by a non-authorized individual can cause a loss of information, research data, confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to Texas Tech University.

All IT Security Policies, including password policies, are available for viewing online at www.infotech.ttu.edu/security.

Selected excerpts from the Password Policy:
• All passwords, including initial passwords, must be constructed and implemented according to the criteria for passwords contained herein
• Individuals must not circumvent the Password Policy for the sake of ease of use.

• Passwords must not be divulged to anyone.
• If the security of a password is in doubt, the password must be changed immediately.
• Passwords must be changed at least every 90 days.
• Computing devices must not be left unattended without enabling a password-protected screensaver or lock, or by logging off of the device.
• Passwords must have a minimum length of 8 alphanumeric characters and must contain a mix of upper and lower case characters and have at least 1 numeric character. The numeric character must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (/#$/%^&*_+=?/~`;:,<>|).
• Passwords must not be reused for a period of one year.
• Your password should be difficult to guess but easy to remember. Substitute numbers or special characters for letters. (But do not just substitute) For example:
  • livefish - is a bad password
  • l1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and is substituted by 1’s can be guessed
  • l1v3f1sh - is far better, the capitalization and substitution of characters is not predictable

In the next two months, the IT Division will begin a password expiration process that will require the changing of eRaider passwords every ninety (90) days. Prior to the expiration, you will receive reminder notifications. In addition, you will be provided the opportunity to change your password when you authenticate.

Quick Tips for the life of your computer:
1. Install updates for your operating system (OS).
2. Update software and antivirus programs to the most current version.
3. Install antivirus software configured to scan your system frequently.
4. Take advantage of educational opportunities to keep your skills current.
5. For assistance contact IT Help Central at 742-HELP (4357).

Contributions by: Katherine Austin Stalcup, J Stalcup, Lori Hefley, Joshua Harrison, Amy Boren, Carlene Van Stone, and Scott Dean.
Safe Computing Practices Committee: Katherine Austin Stalcup, Shannon Cepica, Scott Hall, J Stalcup, Eric Burrell, Lori Hefley, Tony Castle, Darrell Bateman, and assistance from IT Division Directors and other staff.