Looking to the Future

Information Technology Division | Bulletin
vol.2 no.8 | July 2006

Message from the CIO
As we prepare for the always hectic fall semester, this is a good time to review IT Policies relevant to your work at the University. In this issue, we are highlighting “hot topics” that have surfaced in our educational events in the last year. Thanks to our expert panelists from the recent copyright and intellectual property roundtable (Lance Anderson, J.D., Wes Cochran, J.D., Susanne Moore, R.N., J.D., and Marina Oliver), we are providing a synopsis of key copyright principles. The IT Division wishes you a fun and relaxing summer and encourages you to practice Safe Computing throughout the year.

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

An Overview of Copyright Ownership
Contrary to popular belief, copyright ownership does *not* require a notice of ownership or other formalities. In fact, in the absence of an explicit copyright waiver, you should presume that the work is copyrighted. The following rights are solely assigned to the owner of the copyrighted material:

• Reproducing the work
• Developing derivative and adaptive works
• Distribution of the work
• Public performance
• Public display
• Digitally transmitted public performance

These rights exist without regard to possession. For instance, purchasing a music CD (possession of the material) does not give you copyright ownership rights. As such, copying, distributing, and converting are prohibited without express permission from the copyright owner. In the case of a music CD, the copyright owner is typically the recording company.

Fair Use and Copyrighted Materials
Internet-based technologies have made it easy to download and use files located on the Internet. However, we caution that just because the technology allows you to possess a copy of text, music, or video, it does not mean you have the legal right to do so. Congruent with precepts of free speech, the Fair Use Doctrine states that the public may use portions of copyrighted materials for the purposes of commentary or criticism (Copyright Act of 1976, §107). The judicial system has measured fair use in terms of the following aspects:

• The purpose and character of the use
• The nature of work
• The amount and substantiality of the portion used
• The effect of the use on the potential commercial market
• The intention of the user that may persuade a judge or jury

The following principles can be used when determining if your use falls within Fair Use guidelines:

• Factual works are less scrutinized because of the obvious benefit to the public
• Unpublished works have limited Fair Use; the process of publication opens the work to public scrutiny
• The less you take of the work, the more likely your use will be considered Fair Use
• If your use deprives the owner of income, it will not be considered Fair Use
• If your use can satisfy demand for the original work, it will not be considered Fair Use

If you use a copyrighted work to create a derivative work, Fair Use guidelines will apply if you have transformed the work with new meaning or if you have added value to the original work.
IT Security Policies
The TTU IT Division collaborated with representatives from the University community and the IT Advisory Committee to establish TTU IT Security Policies aimed at promoting data integrity, system security, and safe computing practices, as required by the Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202. For a comprehensive list for those units that participated please go to www.infotech.ttu.edu/security. These policies are reviewed on an annual basis by the Office of CIO and the IT Advisory Committee and address the following subject areas:

- Acceptable Use
- Account Management
- Administrative/Special Access
- Authorized Software
- Backup-Business Continuity
- Business Partner Access
- Change Management
- E-mail
- Incident Management
- Information/Data Classification
- Internet Use
- Intrusion Detection
- Network Access
- Network Configuration
- Password
- Physical Access
- Portable Computing
- Privacy
- Public Access/Lab Workstation Hardening
- Security Monitoring
- Security Training
- Server Hardening
- Software System Development
- Unauthorized Software
- Virus Detection
- Workstation Hardening

We strongly encourage you to carefully review these policies at the following location: www.infotech.ttu.edu/security. We rely on input from faculty and staff regarding these policies and procedures, as the successful security oversight is a partnership between the University community and TTU IT Division. In the fall we will be providing additional materials for Network Site Coordinators (NSC) as well as a number of educational opportunities addressing various IT security issues. As always, we welcome your input and ask that you send feedback to the Office of the CIO at cio@ttu.edu.

Acceptable Use
The Acceptable Use policy establishes standards for acceptable and non-acceptable activities using Institutional information resources. Examples of information resources include, but are not limited to, computer hardware, computer software, computer networks, electronic files and data, and printed materials.

Highlights of the Acceptable Use policy include:

- Acceptable Use policy applies to all users accessing University information resources, no matter their location or method of access
- Information resources must be used in a way consistent with the mission and objectives of the University and the State of Texas
- Users must only utilize information resources they have been granted access to and must not circumvent security measures or share authentication secrets with anyone else
- Users must be mindful of security and report any potential security violations or weaknesses immediately
- All users must be respectful, courteous, and ethical in their activities
- Users are personally responsible for their behavior on information resources
- Incidental personal use is restricted to authorized users within certain guidelines, and resources may not be used for personal gain
- All use of information resources is governed by local policies and applicable law

To ensure compliance with Acceptable Use IT Security Policy, review the full policy at www.infotech.ttu.edu/security.

ATM/Debit Card Security Practices

- Change your bank account PIN number if you believe your account has been compromised;
- Avoid entering your PIN number on any PIN pad during checkout;
- Do not give your thumb print at retail stores;
- Check your accounts regularly and report any fraudulent activity immediately to your bank.

Contributions by: Katherine Austin, Ph.D., K. Lance Anderson, J.D., J. Wesley Cochran, J.D., Eric Burrell, Lori Dudley, Joshua Harrison, and Carlene Kelly.

Safe Computing Practices Committee: Sam Segran, Katherine Austin, Ph.D., Shannon Cepica, J Stalcup, Darrell Bateman, Allen Young, Scott Hall, Eric Burrell, Lori Dudley, Alvin Mills, Tony Castle, and assistance from IT Division leadership and staff.