Important “To-do” Reminders for Departments During Employee Transitions

Employees transition to other Texas Tech departments or away from the University throughout the year. Managers are responsible for removing employee access to information resources when employees leave a current position.

Routine Transitions
The Enterprise Application Security (EAS) group, a unit in the Information Systems department of the Texas Tech System IT area, manages access to Banner systems. When an employee transitions from one Texas Tech University department to another, the employee automatically loses current Banner privileges and the new manager must contact EAS to reestablish Banner connection privileges. Managers can email EnterpriseAppSecurity.is@ttu.edu or visit Bugs.itis.ttu.edu to submit a request.

Most information resources at Texas Tech University are accessed through eRaider, in line with TTU IT Security Policy. eRaider accounts of employees that enter and leave the University are automatically added/removed upon completion of ePAF creation/termination processes.

Critical, Security Sensitive Transitions
In situations where immediate removal of central computing access (eRaider, Banner, Central Servers) is critical, managers should contact the TTU Office of the CIO at (806)742-5151 for assistance.

In addition, areas and units should remove access to internal departmental resources immediately, and review all employee access privileges periodically (e.g. annually). Some examples of these information resources include:
- Network Site Coordinator access;
- Department servers;
- Web servers and web pages;
- Local applications;
- Hosted services and applications; and
- Departmental file shares.

Let’s work together to protect TTU information resources.

Message from the CIO
Summer is here! To celebrate the festive summer months, we are focusing this bulletin on new and exciting technologies available to faculty, staff and students. In this issue we highlight Undergraduate Education’s new scheduling software for academic advising appointments, TimeTrade. Another new service coming to TTU is “WEPA@Tech” - TTU Mobile Printing Solutions – new wireless printing stations. Special thanks to the academic advisors who assisted Undergraduate Education and IT with the TimeTrade evaluation, and to Communications & Marketing for their collaboration with WEPA. The IT Division is also excited to announce that we will now be able to provide SPSS in a virtualized environment. In this issue, we also provide Reminders for Employee Transitions, and present more Computer-Based Training courses. Lastly, we provide you with tips on Safely Using USB Drives. Enjoy your summer!

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

SPSS on the Go!

The TTU Information Technology Division offers virtualized IBM SPSS statistical analysis software for access on and off campus. This will provide you the opportunity to use this powerful tool where and when you need it, without installing the software on your system. TTU IT has been working in partnership with the College of Education to pilot the service. To start using the virtualized SPSS environment, go to http://citrix.ttu.edu to download a utility. Please note that we are still evaluating, modifying, and calibrating the services. Look for further information coming soon to TechAnnounce!

Highlights:
- The IT Division has licensed the rights to deliver the SPSS software using application virtualization technologies;
- The Citrix receiver used to access virtual SPSS can be installed on a wide variety of devices, including; desktops, laptops, tablets, and smart phones; and
- The software will run on IT Division servers dedicated to this project, providing user experience and interaction equivalent to having the software on your device.

For assistance or questions concerning this service, please contact IT Help Central at (806) 742-HELP or ithelpcentral@ttu.edu.

CBT - Computer-Based Training is so much more than “learning about computers”

With over 5,300 courses in the TTU catalog, you should find at least one course topic that interests you and adds to your skill set. In this issue, we highlight courses for personal development within the workplace.

Available topics include:
- Living a Balanced Life;
- Effective Time Management;
- Business Ethics;
- Critical Thinking Essentials; and
- Problem-Solving and Decision-Making Strategies.

You can find these and other communication skills in the Personal Development Curriculum in the Business Skills set. You can search the inventory for your own training needs. Browse the catalog at www.cbt.ttu.edu to see all the course topics available to you – anywhere, anytime, for any Raider.

Introducing . . . New Academic Advising Scheduling Software

The TTU IT Division, in collaboration with the Division of Undergraduate Education and Student Affairs, conducted an evaluation of various software tools for academic advisors. One of the products selected by TTU academic advisors, TimeTrade, enhances communication between advisors and students, allowing for flexible, online appointment scheduling. TimeTrade will make student-advisor interactions more efficient, convenient, and streamlined for both groups.

Advising appointments will now be scheduled through email or at www.ttu.timetrade.com. An added feature of TimeTrade is instant appointment confirmation, and reminder emails for both the academic advisor and the student. For more information or specific questions regarding TimeTrade, please contact IT Help Central at (806)742-HELP (4357) or www.ithelpcentral.ttu.edu.
A new form of printing has made its debut in the Advanced Technology Learning Center (ATLC) in the west basement of the Library building. **WEPA - Wireless Everywhere, Print Anywhere** - is a cloud printing solution that will be available across a network of wireless touch-screen printing kiosks.

- Four kiosks are available in the ATLC to allow students and others to print directly from the ATLC lab computers, personal laptops or desktops, mobile devices, and USB flash drives.
- Customers can install WEPA print drivers on personal systems or apps for mobile devices, choose to submit their documents to WEPA@Tech (cloud), and then go to the nearest kiosk to print.
- The Texas Tech University community will pay for printing using their Raider Card. Faculty, staff, and students can deposit funds via the TTU ID Office or through the ID Office website, [http://www.raidercard.ttu.edu](http://www.raidercard.ttu.edu). (Please note TTU will no longer have the ability to provide printing credits each semester.)

Please visit the ATLC to explore the possibilities of cloud printing with WEPA! Once this pilot is successful, it will be made available to key areas on campus and will bring the latest innovations in distributed printing services to TTU.

**USB Flash Drive Safety**

USB flash drives also called jump drives or thumb drives - have gained popularity due to their storage capacity, simplicity, cost, and portability. Additional advantages of flash drives are that they use little power, have no fragile moving parts, are less susceptible to scratches and dust than discs, and they are re-writable. These properties make them suitable for transporting data from place to place, and keeping your data readily at hand.

The biggest disadvantage to these mobile storage devices is they can be easily stolen or lost, and thereby vulnerable to data theft. USB flash drives provide convenience, but unless you take adequate security measures, the information is not only vulnerable to data theft, but could lead to the disclosure of sensitive or private information.

The IT Division suggests these tips for safe usage of USB flash drives:

- Carefully consider the data you are transporting on your flash drive and weigh the implications of possibly losing that information, or transporting it in another, more secure, way;
- Use passwords and encryption to help secure the information on your flash drive; and
- Remember to back-up your data in case your USB flash drive is lost or stolen.

Lastly, do not plug an unknown USB drive into your computer. If you find a USB drive, don’t connect it to your computer to view the contents or identify the owner. It is possible that malware may be installed on the device that could infect your computer. According to a report by Avast Software (2010), one out of every eight malware attacks involves an infected USB device. The attacks often exploit the Windows AutoRun feature, that automatically runs executable files. AutoPlay begins reading from a drive as soon as you insert media into the computer -- this has become a popular form of spreading malware. The IT Division encourages you to disable “AutoRun” or “AutoPlay” on your system. Instructions can be found at [http://askitt.ttu.edu](http://askitt.ttu.edu), by entering “AutoRun” or “AutoPlay” into the search box.

If you feel your system has contracted malware from a USB drive or have additional questions regarding malware, please contact IT Help Central at (806)742-HELP (4357) or visit [www.ithelpcentral.ttu.edu](http://www.ithelpcentral.ttu.edu).