Benefits of TechMail Improvements: Mailbox Default Size Increases

As you may be aware, the TTU IT Division has enhanced our spam management strategies in the last year. A main benefit of these improvements is our ability to process mail more efficiently, thus increasing available storage space. Our ability to reject known spam mail affords us the opportunity to increase your mailbox size to 1 GB from the current default limit of 100 MB. In addition, we recently upgraded the TechMail servers, allowing us to more efficiently manage our current resources and to enhance e-mail features. We will be increasing the size of all TTU mailboxes this fall; the increase will be transparent and mail services will not be interrupted. As a further means of efficiently managing storage resources, please note that after fifteen (15) days, items in your “Deleted Items” folder will be automatically removed by the mail system.

Over the next few weeks, we will also be changing the mail server settings to automatically purge Junk E-mail folder items older than thirty days. We encourage you to routinely check your Junk E-mail folder for mail that you wish to retain.

You may find the following resources useful to learn more about efficiently managing your email and taking advantage of the new collaboration tools:

- Mail archiving instructions and options: http://www.depts.ttu.edu/ithelpcentral/solutions/XP_autoarchive.php
- Technology Support Outlook ShortCourse: http://www.depts.ttu.edu/itts/training/shortcourses
- Technology Support ShortCourse on Live Meeting/Communicator: http://www.depts.ttu.edu/itts/training/shortcourses
- Computer Based Training (CBT) Modules on Outlook and Communicator: http://cbt.ttu.edu

For assistance with e-mail archiving, please visit: http://www.depts.ttu.edu/ithelpcentral/solutions/XP_autoarchive.php or contact: IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu or online at www.ithelpcentral.ttu.edu.

Protecting Institutional Information Resources and Data

As employees of a state institution and in the course of our work duties, we all have a responsibility to protect institutional information resources and data, especially confidential information, such as social security numbers, student grades, home addresses, financial information, etc. As we begin a new semester, we would like to take this opportunity to highlight information that has been shared frequently with the campus community through our IT bulletins, TechAnnounce, Do You Know About series, and our IT educational events. Information Technology resources include hardware, software, and data, including the information posted to University websites (where our published information should be accurate, timely, and congruent with TTU IT Security policies). Please review the relevant TTU IT Security policies at http://www.depts.ttu.edu/infotech/security, specifically, the policies on Acceptable Use, Information/Data Classification, and Privacy that address individual’s responsibility to safeguard confidential data.

For those who manage computing systems, you have additional responsibilities associated with safeguarding data under your purview, regardless of whether you inherited a system or managed it from inception. We ask that you carefully review applicable TTU IT Security policies, such as Account Management, Backup-Business Continuity, Incident Management, Multi-Functional Device Hardening, Password, Physical Access, Security Monitoring, Server Hardening, and Workstation Hardening. We also ask that you familiarize yourself with the following TTU Operating Policies (http://www.depts.ttu.edu/infotech/ops/).

- 52.01 - Information Technology Operations
- 52.02 - Infringement of Copyrights in Information Technology
- 52.03 - Obtaining Data Network Services
- 52.04 - Information Technology Security
- 52.05 - Electronic and Information Resources Accessibility
- 62.06 - Payment Card Processing By University Departments
- 62.14 - Red Flag Rules
- 30.22 - Guidelines For The Educational Use Of Copyrighted Works
- 48.04 - Cellular Telephone Policy

(continued on back)
Securing Confidential Data on Your Laptop: Portable Device Encryption Software Now Available

Portable computing devices are becoming increasingly powerful and affordable. Small size and functionality are making these devices ever more desirable to replace traditional desktop devices in a wide number of applications. However, the portability offered by these devices may increase the security exposure to the customer.

Texas Tech University’s Portable Computing Policy indicates that confidential or sensitive data should not be stored on portable computing devices. However, in the event that you are a professional who needs to store confidential data on your laptop and have no viable alternative to local storage, all confidential or sensitive Texas Tech University data must be encrypted using approved encryption techniques.

To facilitate compliance with state regulations, including TTU Security Policies, mandating that confidential data on portable device be encrypted, the TTU IT Division will provide licenses for PGP Whole Disk Encryption (WDE) software for Windows and Mac operating systems.

The Portable Computing Policy can be reviewed at http://www.depts.ttu.edu/infotech/security/docs/portable_computing.php. If you are a professional who needs local storage of confidential data on your laptop and would like to request a copy of PGP WDE, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu or online at www.ithelpcentral.ttu.edu.

Contributions by: Katherine Austin, Ph.D., Shannon Cepica, Mark Holwerda, Yung Ng, J Stalcup, Britta Tye, Nicole Weatherly, Laura Webb, and Allen Young.

Safe Computing Practices Committee: Sam Segran, Katherine Austin, Ph.D., Darrell Bateman, Pulin Bhatt, Shannon Cepica, Paco Diaz, Scott Hall, Mark Holwerda, Michael Horton, Danny Mar, Alvin Mills, Yung Ng, Mike Simmons, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.