THE UNIVERSITY OF TEXAS OF THE PERMIAN BASIN

Security Requirements For UTPB Computer Users

Rev 6-1-04

1. Do not open any files attached to an email from an unknown, suspicious or untrustworthy source.

2. Do not open any file attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. The safest approach is to confirm that the apparent sender really sent the message/attachment. Many viruses can replicate themselves through e-mail if an infected attachment is opened.

3. Do not open any files attached to an email if the subject line is questionable or unexpected.

4. Do not use e-mail attachments unless your message really needs an attachment. For example, if your message consists of only plain text, send the message as a plain text message, not as a Word attachment. This approach is much more efficient and eliminates the potential for an infected attachment. E-mail isn't free. Every message consumes network and disk resources. Use attachments only when necessary and keep message size as small as possible.

5. Do not use 3rd party "enhancements" to your e-mails. This includes "cute" smiley face icons, special backgrounds and special signature blocks. These items contribute little to the utility of your message, needlessly increase the size of your message and represent potential virus infection or security problems. Simple text messages are the most efficient and least likely to provide an infection path for virus activity.

6. Delete chain emails and junk email. Do not forward or reply to any of them. This type of email is called "spam", which is unsolicited, intrusive mail that slows down the network. Responding will only result in more junk mail. Do not click on any links that offer to remove you from a spammer's mailing list. This lets them know that the address is operational. They may or may not remove you from their mailing list, and they will probably sell your e-mail address to other spammers. Be careful about entering your email address in Web sites that require you to register in order to access the features available on the Web site. Some sites will sell your email address to spammers. You may want to read the site's privacy statement before submitting your information.

(continued on page 2)

4901 E. University · Odessa · Texas 79762-001 · (432) 552-2415 · Fax (432) 552-2416

Security Requirements For UTPB Computer Users (continued)

7. Be sure that you understand University rules, state laws and federal laws governing the sending of Unsolicited Bulk E-Mail (UBE) BEFORE you consider using any form of mass e-mail facility. State and federal law now place specific requirements and restrictions on UBE senders.

8. **DO NOT** download software or files from the Internet. This includes cute screen savers, special backgrounds, special cursors, special tool bars, performance "enhancers", or ANY of the ten million pieces of junkware that beg to be downloaded daily. While some of these "free" applications may appear to offer attractive functionality, many of these items are of questionable origin and almost all of them rob your system of performance. Some may represent serious security threats to the university network. Peer-to-peer file sharing utilities such as Napster, Gnutella, iMesh, Audiogalaxy Satellite, KaZaA and others are potentially serious security risks and should not be used on university computers.

9. Update your anti-virus software regularly. Over 500 viruses are discovered each month. Most anti-virus software consists of two components; the scan Engine and the virus Profiles. Since the virus world is very dynamic you should update the virus Profile information frequently. Most university systems are configured to do this update automatically. The specifics of how this is done depend on the particular anti-virus software being used.

10. Respect the confidentiality of information. Some of the information handled by university employees is protected, confidential information and should be handled accordingly. Social Security numbers, academic records and medical information are all protected by various state and federal laws. Be sure that you understand the legal restrictions associated with the information you handle. For example, do not send confidential information through e-mail.

11. Do not share passwords. This applies to computer passwords and voicemail passwords. The UTPB Acceptable Use Policy requires that passwords be used only by the assigned account holder. Do not divulge your passwords to anyone. Never provide your password to someone over the telephone. Use good security practice and change your passwords often.

12. Do not cache passwords. Some applications ask if you would like to have your password "remembered" to save typing in the future. While having the application "remember" your password is a convenient "feature" this is very poor security practice provides anyone with physical access to your computer easy access to your identity and your information.

13. Back up your DATA files on a regular basis. If a virus destroys your local data files, at least you can replace them with your back-up copy. You should store your backup copies in a separate location from your work files, a location that is preferably not on your computer. Store your data files in a common folder/location such as "My Documents" to make backup easier.