Tennessee State University – Information Technology Policy

XIV. Password Policy (revised 5/2009)

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly constructed password may result in the compromise of an e-mail or computer access account or even the entire TSU network.

All TSU students, employees, contractors, and vendors with access to TSU computer and network systems are responsible for taking the appropriate steps, as outlined in this policy to select and secure their passwords.

This password policy will apply to the following systems: the TSU network, TSU wireless network, myTSU, Exchange e-mail, TSU website accounts, screen saver protection, SciQuest purchasing system, eLearn (D2L) system, and INB Banner, and any other computing or network resource used on the TSU campus. The strong password policy may not be enforced on all systems simultaneously but as time and platform specific strong password policies can be applied.

This policy establishes the requirements for creating strong passwords, the protection and management of passwords, and the frequency that passwords are to be changed.

Creation of Strong Passwords

The use of strong passwords is necessary to thwart would be computer hackers attempting to "guess" your password using what are known as "password crack" programs.

Strong password construction criteria includes:

- Must contain a minimum of eight characters
- Must use a combination of upper and lower case letters
- Must use at least one numeric and one special character. e.g., 0-9,
- !@#$%^&*()_+|~- =\`{}[]:";'<>?,./)
- Must not be a word in any language, slang, dialect, jargon, etc.
- Must not be based on personal information, names of family, etc.

Password Management and Protection

- Passwords must not be inserted into email messages or other forms of electronic communication.
- Do not use the same password for TSU accounts as for other non-TSU access (e.g., personal ISP account, option trading, benefits, etc.).

- Do not share TSU passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential TSU information
- Passwords should never be written down or stored on-line
- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not reveal a password to your boss
- Do not talk about a password in front of others
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members
- Do not reveal a password to co-workers while on vacation
- Do not use the "Remember Password" feature of applications (e.g. Outlook) that remembers your password when the username is entered.
- Do not write passwords down and store passwords anywhere in your office
- Do not store passwords in a file on ANY computer system including mobile devices without encryption
- Change passwords at least once every six months

Password Reset Frequency

Passwords must be changed at least every six months. Some systems periodically force user password resets by expiring the password.

General Password Construction Guidelines

Weak passwords have the following characteristics:

- Contains less than eight characters
- Forms a word found in a dictionary (English or foreign) or is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "TSU" or any derivation
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321
- Uses any of the words referenced above spelled backwards
- Uses any of the above preceded or followed by a single numeric digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Not a word in any language, slang, dialect, jargon, etc.
- Not based on personal information, names of family, etc.

If a password compromise is suspected, report the incident to CIT and change all passwords.

If someone demands a password, refer them to this document or have them call the Helpdesk. (**615-963-7777**)

Techniques for creating and remembering strong passwords

Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.