Tennessee Technological University
Policy No. 852

Password Management

Effective Date: January 1, 2014

Policy No: 852
Policy Name: Password Management Policy
Policy Subject: Password Management
Date Revised: January 1, 2014

I. Purpose

This policy provides guidance on the creation, use and maintenance of account credentials and passwords used to access Tennessee Technological University's information technology facilities and resources. This policy complements and supports the compliance of Tennessee Board of Regents Policy 1:08:00:00, Section 7.1.A and the State of Tennessee Enterprise Information Security Policies.

II. Review

This policy will be reviewed every 365 days or whenever circumstances require review, whichever is earlier, by the Chief Information Security Officer with recommendations for revision presented to the Chief Information Officer and the ITC.

III. Scope

This policy shall apply to all persons and organizations using the information technology facilities and resources owned, leased, or administered by the University, including all persons employed (either as full-time, part-time, or temporary employees, or as independent contractors) by the University or Tennessee Board of Regents, and to all students enrolled at the University, and alumni. This policy replaces all previous TTU password policies.

IV. Policy

A combination of a personal user login ID for identification and a unique password for authentication will be required of all users before they are allowed access to the Tennessee Technological University network and systems. Passwords will be used for authentication of access to all Tennessee Technological University network and systems except where stronger authentication methods (such as biometric authentication or two-factor authentication) are deemed necessary. The effectiveness of passwords to protect access to TTU's information directly depends on strong construction and handling practices.

V. Procedures

A. Password Construction

All users must construct strong passwords for access to all TTU networks and systems, using the following criteria:

1. Must be a minimum of eight (8) characters in length, at least five (5) of which should be unique

2. Must be composed of a combination of the following four types of characters.

a. At least one uppercase alphabetic character (A-Z)

b. At least one lowercase alphabetic character (a-z)

c. At least one numeric character (0-9)

d. At least one non-alphanumeric character

(~, !, @, #, $, %, ^, &, *, -, =, +, ?, [,], {, })

3. Must not consist of:

a. Dictionary (identifiable) words in any language

b. Personal information, such as birthdays, phone numbers, family names, or pet names

c. Passwords which are the same as the user ID

d. Tennessee Technological University, TTU, or any derivation

e. Common letter or number patterns

f. Variations of old or related passwords used within the last eight (8) passwords

Strong passwords can be difficult to remember. One method for creating a strong password that can be more easily remembered is to select a phrase that is meaningful to you but not known by others, use the first letter of each word in the phrase, and add other special characters, numbers, etc.

For example, 2 years that will change your life! becomes the password 2ytwCyl! (Please do not use this example as your password.)

Where possible, the information system or application will enforce strong password use.

B. Password Management

The following requirements apply to password management:

1. Storage and Visibility:

a. Passwords should be memorized, not written down or saved on your computer or network file storage.

b. Passwords must not be stored in a manner which allows unauthorized access.

c. Passwords will not be visible on a screen, hardcopy, or other device.

d. Passwords will not be stored in a clear text file. This includes storage of passwords in spreadsheets, configuration files, database files, application code, and system directories. Any such passwords must be encrypted if they are required.

e. Passwords will not be sent via unencrypted e-mail. Neither TTU faculty/staff nor TTU student e-mail is encrypted.

2. Changing Passwords:

a. Users must change their passwords according to the schedule below:

i. TTU Domain accounts & INB: at least every 90 days

ii. Administrative & Privileged Accounts – all: at least every 30 days

iii. Eagle Online & Self-Service Banner: at least every 180 days

b. Users should never rotate through a list of favorite passwords.

c. Applications and systems should require that new passwords cannot be the same as the eight (8) previously used passwords.

3. Passwords must be changed immediately if any of the following events occur:

a. Unauthorized password discovery or usage by another person

b. System compromise (unauthorized access to a system or account)

c. Insecure transmission of a password

d. Accidental disclosure of a password to an unauthorized person.

e. Replacement of an account user with another individual requiring access to the same account when account role cannot be re-assigned.

f. Password is provided to the end-user by the system administrator when establishing a new account or resetting the password.

4. Password Protection:

a. Passwords must never be transferred or shared with others.

b. Users should never respond to any email requesting his or her password.

c. Passwords must not be transferred electronically over the internet or intranet using insecure methods.

d. When it is necessary to disseminate passwords in writing, the recipient will protect the written password from unauthorized access. After memorizing the password, any written records must be destroyed.

e. When transmitting a password orally, measures should be taken to ensure that the conversation is not overheard.

f. Use of the "Remember Password" feature on many applications is highly discouraged.

5. Password Protection - System Administrators:

ITS personnel may need to create or disseminate passwords to others and must use a method of password creation that provides the password only to the intended end-user.

ITS operations must implement the following to deter password cracking:

a. An automated method to mitigate "brute force" password attacks should be used. For example, some systems will lock an account for a few minutes after several failed login attempts.

b. Logging must be set up to record all failed login attempts and selected successful attempts as well.

6. Password Protection – Application Developers:

a. Application developers must use secure authentication methods, whenever possible.

b. Creating applications which store passwords should be avoided. If password storage cannot be avoided, developers must ensure that applications do not store passwords in clear text or in a readily decrypted form.

c. Applications should support unique logins. Password sharing should not be allowed.

VI. Interpretation

The Chief Information Security Officer has final authority to interpret the terms of this policy.

VII. Citation of authority for policy

TBR Policy 1:08:00:00; State of Tennessee Enterprise Information Security Policies