Taft College

Procedure: Strong Password

I. Scope
Procedures outlined in the following document apply to all Taft College faculty, staff, students, visitors, and contractors. This policy applies to all academic, administrative, networking and microcomputer resources installed at all Taft College (TC) locations.

In addition to the policies listed below, all users are subject to existing state and federal laws along with institutional AP 3720 concerning the use of computers, email, and the Internet.

II. Definitions

*Password* - A password is a string of characters used for authenticating a user on a computer system.

*Privileged Account* – Privileged accounts are those accounts with administrative or root access to a system and used for the administration of an application or database. Example: Oracle database administration, Banner, etc.

*System Account* - Accounts used for automated processes without user interaction or device management.

III. Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts including network login, email accounts, and web accounts. Poorly constructed passwords may result in the compromise of Taft College’s entire network and its data. Given the threat to personally identifiable information, this procedure is provided as one means to safeguard that information.

IV. Purpose
The purpose of this procedure is to establish a standard for the creation, use and protection of passwords by Taft College faculty, staff, and students. This policy also sets forth the frequency of change required for passwords.

V. Procedure

A. General
All users of Taft College information systems will have a unique user identification and password.

B. Passwords
1. User Passwords - Change all user level passwords (network logon, portal, etc.) every semester.

2. Students are exempt from password changes as accounts are auto generated by existing systems.

3. Privileged Accounts – Users with privileged accounts must change their passwords every 180 days.

4. System Accounts – System Account passwords are not required to expire, but must meet the password construction requirements defined in this policy.

C. Other

1. Vendor provided passwords must be changed upon installation using the construction standards in this policy.

2. User accounts that have system-level privileges granted through group membership or programs such as “sudo” must have a unique password from all other accounts held by that user.

3. Where Simple Network Management Protocol or SNMP is used, the community strings must be defined as something other than the standard defaults of “public,” “private” and “system” and must be different from the passwords used to log in interactively. A keyed hash must be used where available and technically feasible (e.g. SNMPv2 or v3).

4. Passwords must not be sent by email messages or other forms of electronic communications. Exception: Sending an initial password that must be changed on login.

5. All user-level and system-level passwords must conform to the guidelines for strong passwords as described later in this document.

6. Password parameters will be set to prevent users from reusing the past ten (10) passwords.

7. The minimum age duration for passwords will be one day.

8. Password grace periods will be thirty (30) days during which the user will be warned that password is due to expire.

Accounts will be locked after three (3) attempts. User must contact the Help Desk or Administrative Systems to reset.
Faculty and staff desktops will be locked after 60 minutes of inactivity requiring a logon using their password.

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

a. Unauthorized password discovery or use by another person.

b. System compromise... any unauthorized access to a system or account.

c. Insecure transmission of a password.

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

e. Status changes for personnel with access to privileged and/or system accounts.

VII. Guidelines - General Password Construction

A. Weak passwords have the following characteristics:

1. Contains fewer than eight (8) characters

2. Is a word found in a dictionary (English or foreign)

3. Common use words such as names of family, pets, friends, co-workers, fantasy characters, computer terms, commands, sites, companies, hardware, or software should not be used. Any of the above preceded or followed by a digit.

B. Strong Passwords have the following characteristics:

1. Contain a minimum of eight (8) characters consisting of three (3) of the following four (4) character categories. These will be enforced.

   a. English upper case characters (A-Z)

   b. English lower case characters (a-z)

   c. Base 10 digits (0-9)

   d. Non alphanumeric characters (~!#$%^*_~)

   NOTE: Banner and Oracle have restrictions on the use of special characters. Do not use the following for such accounts: ` @ $ ^ & ( ) ; " < >

2. The following are recommended:
a. Is not a word in any language, slang, dialect, or jargon, etc.

b. Is not based on personal information.

C. Use of Passphrases
Passphrases are longer versions (23 character minimum) of passwords and are therefore inherently more secure. A passphrase is typically composed of multiple words and therefore provides more security against “dictionary” attacks. An example is “This May Be One Way to Remember” and the passphrase could be “ThisMaybeOneWaytoRemember” or reduced to “TmB1w2R!” Another example: “IamtheCapitanofthePina4”. According to the National Institute of Standards and Technology (NIST) this passphrase of at least 23 characters contains a 45 bit strength.

Use of passphrases is encouraged as an alternative to passwords because they are generally easier to remember.

VIII. Password Protection Standards

A. Do not use the same password for Taft College accounts as used to access non-Taft College accounts (e.g., personal Internet Service Providers such as MSN, Yahoo, Google, trading accounts, banking accounts, etc.).

B. Do not share your Taft College account information with anyone, including administrative assistants, secretaries, or supervisors. All passwords are to be treated as sensitive and confidential Taft College information.

C. Here is a list of don’ts for password security:

1. Don’t reveal a password over the phone to anyone.
2. Don’t reveal a password in an email message. An exception is transmittal of an initial or reset password that must be changed upon access.
3. Don’t reveal your password to your boss.
4. Don’t talk about your password in front of others.
5. Don’t hint at the format of your password… “my family name”, etc.
6. Don’t reveal your password on questionnaires or forms.
7. Don’t share your password with family members.
8. Don’t give your password to someone when leaving for vacation.
9. Don’t use the “Remember Password” feature in applications.

10. Don’t write your password on a post-it-note, leave it under your keyboard, or leave it “hidden” somewhere in your office.

11. Don’t store your password on another device such as a Personal Digital Assistant (PDA) or USB drive without encryption. You may use a password storage utility as long as it encrypts the stored data; in addition, ensure it is protected by a strong password.

D. Report the incident to the Information Technology office immediately and change all passwords if you suspect your password has been compromised.

E. The Office of Information Technology or its designee may periodically run password “cracking” or “guessing” utilities to assess the compliance of this policy. If the password is “guessed” or “cracked” during this scan, users must change passwords.

F. Where technically feasible, provide role management such that one user can perform the functions of another user without having to know the other user’s password.

IX. Enforcement and Compliance
Any employee found in willful violation of this policy may be subject to disciplinary action covered under the West Kern Community College District’s AP 3720.

X. Responsible Party
The Executive Director of Information Services shall be responsible for development and maintenance of this procedure for issuance by the superintendent.