# USER PASSWORD SELECTION AND PROTECTION STANDARDS PROCEDURE (TCH-P028)

Clarksville-Montgomery County School System

The online version of this procedure is official. Therefore, all printed versions of this document are unofficial copies.

## 1.0 SCOPE:

1.1 This procedure outlines the process for creation of passwords, protection of passwords, and frequency of change.

## 2.0 RESPONSIBILITY:

2.1 Systems Administrators

2.2 Programmers

## 3.0 APPROVAL AUTHORITY:

3.1 Chief Technology Officer

## 4.0 DEFINITIONS:

4.1 Encryption: The process of obscuring information to make it unreadable without special knowledge such as a passkey.

## 5.0 PROCEDURE:

5.1 Users will select passwords following the Guidelines in 5.2 and Password Protection Standards in 5.3.

5.2 **Guidelines**

5.2.1 Passwords must meet the following minimum requirements:

5.2.1.1 At least twelve characters in length;

5.2.1.2 Shall not contain the user's account name or the user's first, middle, or last name;

5.2.1.3 Must not be one of the three most recently used passwords.

5.2.1.4 Must contain characters from three of the following four categories:

- English upper-case letters (e.g., A through Z)
- English lower-case letters (e.g., a through z)
- Base 10 digits (e.g., 0 through 9)
- Non-alphanumeric characters (e.g., !$%#)

5.3 **Passwords Protection Standards**

5.3.1 Do not include passwords in email or other forms of electronic communication (with the exception of inputting a technology work order).

5.3.2 Do not use the same password for CMCSS accounts as for non-CMCSS accounts (e.g., personal bank account, personal email account, etc.).

5.3.3 Do not share CMCSS passwords with anyone, including administrative assistants or bookkeepers, with the exception of your direct supervisor or the CMCSS Technology Department, upon their request (ref. HUM-A034).

5.3.4 If anyone other than your supervisor demands a password, refer them to School District Communication System Usage Policy (ref. HUM-A034) or have them call the CMCSS Technology Department.

5.3.5 Do not share password with family members or friends.

5.3.6 If an account or password is suspected to have been compromised, report the incident to the CMCSS Technology Department and your supervisor and change all passwords.

5.3.7 If a user is away from the computer, that user is responsible for logging out or locking the screen in order to secure their account.

5.3.8 Passwords should not be written down and left in plain sight, such as on a sticky note.

5.3.9 Passwords should not be stored in an electronic file or document, unless the file or document is encrypted and password-protected.

## 6.0 ASSOCIATED DOCUMENTS:

6.1 TCH-A003 User Password Policy
6.2 HUM-A034 School District Communication System Usage

## 7.0 REVISION HISTORY:

| Date: | Rev. | Description of Revision: |
|---|---|---|
| 7/18/11 | IR | Initial Release |
| 9/10/12 | A | Per CTO- updated amount of time to change passwords to “four months”, corrected TCH-A034 to be HUM-A034 under Password Protection Standards, corrected TCH-P003 to TCH-A003 and added HUM-A034 to Associated Documents, added policy title to 5.4.4. Updated logo and formatting. |
| 5/3/13 | B | Update Responsibility to System Administrators, change four months to 120 days, update 5.3.1.1, add 5.3.1.4, delete “is not a single work in any language, slang, dialect, jargon, etc.”, change to Alphanumeric, flow chart removed. |
| 4/20/15 | C | |

| | | |
|---|---|---|
| | | 4.3 changed directions to systems. Reword 5.2.2, add unless tied to active…in 5.2.3, change characters to letters in 5.3.1.3, update 5.3.1.4, 5.4.2 & 5.4.5, remove do not talk about a password under list of don'ts. |
| 1/6/16 | D | Updated password requirements throughout procedure. |
| 2/6/17 | E | Added 2.2. Changes throughout due to new procedures being followed. Please see previous revision dated 4/20/15. |
| 6/2/20 | F | Updates to 5.2.1.1. and 5.2.1.3. |
| 3/17/23 | G | Removed System Level Privileges and Active Directory Account definitions. Updated 5.3.8 |

*****End of Procedure*****