Title: OIT0400 Password Policy

Policy Owner: Chief Information Officer

Responsible Department: Office of Information Technology

I. Overview

The St. Thomas University Password Policy establishes the position that poor password management or construction imposes unacceptable risks to the security of University information systems and resources. Standards for construction and management of passwords greatly reduce these risks.

II. Objective / Purpose

This document describes the acceptable standards for password construction and management.

III. Scope

The requirements in this standard apply to passwords for any computing account on any university computer resource, to the users of any such accounts, and to system administrators and developers who manage or design systems that require passwords for authentication.

IV. Standard

A. Password Construction

a. Minimum Password Length

Passwords shall have a minimum of 8 characters with a mix of alphanumeric and special characters; if a particular system will not support an 8 character passwords, then the maximum number of characters allowed by that system shall be used.

b. Password Composition

Passwords shall not consist of well-known or publicly posted identification

information. Names, usernames such as your Student ID, birthdates, anniversary and phone numbers are all examples of well know identification information that should not be used as a password.

Additional password construction guidelines can be found in Appendix A: Password Construction Guidelines.

B. Password Management

a. Password Storage

Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames.

Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable (such as LastPass), although extreme care must be taken to protect access to said application.

b. Password Expiration

Passwords shall expire every 90 days

c. Password Lockout

After 5 consecutive invalid logon attempts the account shall be locked for 30 minutes.

d. Password History

Users will be prohibited from re-using the last 5 previously used passwords.

e. Password Reuse

Care shall be taken to prevent the compromise of one username/password from compromising the security of multiple systems or resources. The username and

password(s) used for your STU accounts should never be used for any other non-STU accounts and services.

f. Password Sharing and Transfer

Passwords shall not be transferred or shared with others unless the user obtains appropriate authorization to do so.

When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record.
When communicating a password to an authorized individual orally, take measures to ensure that the password is not overheard by unauthorized individuals.

g. Electronic Transmission

Passwords shall not be transferred electronically over the Internet using insecure methods. Wherever possible, security protocols including IMAPS, FTPS, HTTPS, etc. shall be used.

h. Requirements for System Administrators

- **Require Passwords for Login** - Systems shall not be configured to allow user login without a password. Exceptions shall be granted for specialized devices such as public access kiosks when these devices are configured with public user accounts that have extremely restricted permissions (e.g. web only) that are separate from administrative accounts.
- **Changing Password after Compromise or Disclosure** - System administrators shall, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource. Examples of these situations include but are not

limited to: disclosure of a password to an unauthorized person; discovery of a password by unauthorized person; system compromise (unauthorized access to a system or account); insecure transmission of a password; replacing the user of an account with another individual requiring access to the same account; password is provided to IT support staff in order to resolve a technical issue; account password is communicated to a user by the system administrator.

- **Default Passwords -** System administrators shall not use default passwords for administrative accounts.

C. Enforcement and Implementation

a. Roles and Responsibilities

Each University department/unit is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard.

The Office of Information Technology is responsible for enforcing this standard.

b. Consequences and Sanctions

Non-compliance will result in the loss of access to University systems until compliance is achieved.

Any device that does not meet the minimum security requirements outlined in this standard may be removed from the STU network, disabled, etc. as appropriate until the device can comply with this standard.

Appendix A: Password Construction Guidelines

Acceptable Methods to Create a Strong Password

Use a minimum of 8 characters. Generally, the more characters you can use, the harder a password is to be cracked or guessed.

Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use a sentence or saying to create a "passphrase" by using the first letters, capitalization, and special characters as substitutes. For example, "One ring to rule them all, one ring to bind them" may be used to create a passphrase like "1R2rtAor2Bt" that can be used as a very strong password.

Passwords **must include** at least three of the four following types of characters:

- English uppercase letters (A through Z).
- English lowercase letters (a through z).
- Numbers (0 through 9).
- Special characters and punctuation symbols (Example: _, -. +, =,!, @, %, *, &, ", :, ., or /).

Do not use:

- The following characters: \ , ~ or <
- A space or tab
- Reuse of any of your last 5 passwords is prohibited.

Tips for Creating a Strong Password

- Avoid words, numbers, or known or public information associated with you. (e.g. Social security numbers; Names, family names, pet names; birthdays, phone numbers, addresses; etc.)
- Avoid using your login name or any variation of your login name as your password. If your login is 'fredrick', do not use substitution or letter reordering. Examples would be

'fr3dr1ck', where the 3=e and the 1 (one)= i. Alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).

- Avoid using the same character for the entire password (e.g., '11111111') or using fewer than five unique characters.
- Avoid common letter or number patterns in your password (e.g., '12345678' or 'abcdefgh'). They are the first things hackers will test.
- Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=I, 0=O, etc).
- When changing a password, change to an entirely new password. Do not just rotate through a list of favorite passwords.