IT Standard Title:	Password and Passphrase Protection
Standard ID:	US-101
Standard Type	User
Classification	Public
Linked to Policy:	6-604 Information Security Policy
Approved by CTO	2022-08-25
Revision Date(s):	2022-08-18 (Initial)
Effective Date:	2022-08-29
Next Review Date:	Annually
Contacts for Interpretation:	ITS Support Manager, IT Customer Services

1 – Purpose

All Fleming users are responsible for maintaining the security of their Fleming user account(s). The primary method of doing so is to ensure that you have a strong and unique password known only to you.

This document defines the College standard for the creation and use of passwords/passphrases to protect Fleming College user accounts and electronic information.

Fleming College ITS Service Desk is available to assist users with all password/passphrase related questions.

The Chief Technology Officer has issued this user standard under the authority of College Policy 6-600 IT Policy Framework.

2 – Definitions and Acronyms

Password	A series of potentially random letters, numbers, and special symbols. Various techniques are often used to help make them easier to remember, such as, consider using the first letter of each word in a phrase, for example, "I ride my bike to school at 7 AM!" becomes "Irmbtsa7AM!".
Passphrase	A sequence of disconnected words and other characters that is often easier to remember than a long password of potentially random characters. E.g. such “GreenDogSmiles1”.
Single Sign-on (SSO)	An authentication service that allows users to use one set of centralized login credentials to access multiple services.
Multi-factor Authentication (MFA)	A security technology that requires multiple methods of authentication from independent categories of credentials to verify a user’s identity. Most often a

password/passphrase and one additional method is required, such as a code sent by SMS text message or via a smartphone authenticator application.

3 – Password and Passphrase Protection

Passwords and passphrases are common and important ways to access and protect electronic information on almost any type of system, application, or device. The top three ways to keep a password/passphrase safe to protect your account(s) and information are:

1. Create a strong password/passphrase
2. Guard it carefully (e.g., don't share it or write it down)
3. Avoid reusing it for other systems

Consequently, attackers attempting to access information use a variety of tools and techniques to steal passwords/passphrases. Some of these methods include:

- Brute force (guessing easy or common passwords/passphrases)
- Phishing
- Data breaches
- Malware

Following this standard for password/passphrase protection, and related cybersecurity guidance and training will help ensure that your accounts and information remain safe and secure.

Using a passphrase as a mnemonic device is recommended versus a password as passphrases tend to be longer and easier to remember. For the rest of this document, the term password will be used generically to mean password or passphrase.

4 – Creating a Password/Passphrase

A strong password is required to ensure that it can not be easily guessed, even by software that can automate billions of attempts to crack a password.

Length: Use a password with a minimum of ten (10) characters, the more the better. Some Fleming systems do not support passwords longer than thirty-two (32) characters.

Complexity: Use a complex password that contains a mix of at least three (3) character types: upper case letters (A-Z), lower case letters (a-z), numbers (0-9) and symbols (#, !, $, %, @, etc.)

Avoid using a password that replaces a letter with a number, symbol, or other common substitutions, such as "Pa$$word2022" as automated guess programs are very familiar with these common alpha/numeric replacements. Also never use the word "password" or any variant thereof, as part of your password. These are also commonly used and easily guessed.

Name, username, address, date of birth, family members' names, or any other term that can be easily guessed or researched about you online, such as via social media, should not be used to create a password.

Password generation and storage programs should be used to create and manage passwords. See below for recommended password manager applications.

5 – Changing a Password/Passphrase

Passwords for ITS network staff login accounts must be changed every 180 days.

It is recommended that all other passwords are changed at least annually.

When changing a password, do not reuse any previous passwords.

6 – Protecting a Password/Passphrase

Use a password safe or password manager to securely store multiple passwords as it is only then necessary to remember a single master password. See below for recommended password manager applications.

Do not write passwords down. If necessary to write a password down it must be locked away in a secure, inaccessible location such as a safe.

Best practices state that personal passwords, attributed to an individual, should not be shared, even with trusted individuals. Create multiple user accounts with similar permissions as needed instead of sharing passwords.

Fleming ITS staff will never ask for a user's password. Do not respond to emails or phone calls requesting passwords of MFA passcodes even if they appear to be from a trusted source.

Password must be immediately changed if there are suspicions that they could have been compromised. The incident must be reported to the ITS Service Desk.

7 – Single Sign-on (SSO)

Having too many passwords can be a challenge unto itself and creates complexity for the user, often leading to poor password practices.

To help simplify this challenge the College enables many of our systems, services, and devices to use the College's centralized SSO service, as the primary form of identification and authentication, where feasible and supported to do so.

Using a single source of identification and authentication also helps to reduce the amount of account management necessary compared to when disparate login credentials are used.

When considering the use of a new system/service/device at the college, before any purchase, users must work with ITS to review support for SSO and MFA. Depending on the scope, scale, and information sensitivity level of the new system/service, one or both of SSO and/or MFA may be required. Contact the ITS Service Desk to initiate this review.

8 – Touchscreen Interfaces

On touchscreen devices without a full keyboard, it is not practical to use a strong password to lock/unlock the device. Instead, the following means of authentication can be used:

- A biometric control such as fingerprint or facial recognition (preferred)
- A numeric password/PIN that is at least 4 characters long
- A drawn pattern that is reasonably complex

Exercise caution when entering PINs or patterns into touchscreen interfaces as they may be easily overseen by a keen observer.

9 – Multi-Factor Authentication (MFA)

Where available users should enable and use multi-factor authentication (MFA). It may be required and/or enforced in some circumstances. Refer to Appendix B – Security Protections for Information Classification Levels within the College's Information Security Classification Procedure (#6-604A) for more information on MFA requirements.

The following method of MFA are recommended and supported by the College:

Name	Description & Details
Microsoft Authenticator (Mobile Application / Preferred)	Installed on Fleming provided mobile device or personal mobile device. Available for Android and Apple iOS.
SMS Text Message	To a Fleming-provided mobile device or personal mobile device.
Telephone Call	To a Fleming provided phone number, extension, or other personal and direct phone numbers.

10 – Privileged Accounts

Privileged accounts that are used to administer systems, applications, and other services are subject to additional password requirements detailed in the ITS Technical Standard for Privileged Account Management.

11 – Password Manager Applications

A Password Manager (sometimes also called a password safe or vault), is a computer application that provides a secure place to store and access the passwords for different login environments. Password Managers are simple to use because they can be accessed with a single master password.

The master password must be strong to protect the security of the contents within. The master password must be changed at least annually. Users are responsible for remembering the master password. Fleming ITS cannot recover it if lost.

The following password managers are supported and recommended by Fleming ITS.

Name	Description	More Information
KeePass & KeePassXC	Available for Windows, macOS, and Linux, as well as iOS, and Android mobile operating systems. A popular open-source, cross-platform, desktop-based password manager. It stores all passwords in a single database (or a single file) that is protected and locked with one master key.	**Availability:** Anyone **Cost:** Free **Vendor Link:** https://keepass.info/ https://keepassxc.org/ **Type:** Standalone desktop application **Encryption:** AES-256
1Password *** NEW ***	A password manager, digital vault, random password generator, and form filler. 1Password remembers all your passwords for you and keeps them safe behind the one password that only you know. Apps are available for macOS, iOS, Windows, Android, and as a web-browser plug-in.	**Availability:** Enterprise license available to Fleming staff members upon request to IT Support. Students may purchase personal accounts from the vendor at their discretion. **Vendor Link**: https://1password.ca/ **Fleming Service Catalog:** 1Password – Fleming ITS **Type:** Web-based with desktop and mobile applications, and a browser plug-in. **Encryption:** AES-256

12 – Related Documents

- College Policy 6-600 - IT Policy Framework
- College Policy 6-601 - Appropriate Use Policy
- College Policy 6-604 - Electronic Information Security Policy
    - OP 6-604A – Information Security Classification Procedure
    - OP 6-604B – Access Control Procedure

13 – History of Amendments & Reviews

NA