IT Standard Title:	Encryption Requirements
Standard ID:	US-102
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 Procedure Interpretation:	ITS Support Manager, IT Customer Services

1 – Purpose

Encryption is the process of making information unreadable to protect it from unauthorized access. After information has been encrypted, a secret key or password is needed to unencrypt it and make it readable again.

This document defines standards that all users must comply with for encrypting devices and files, used to access and store Fleming electronic information so that the information is protected from unauthorized access. Refer to Fleming College Information Security Classification Operating Procedure (6-604A) to determine when and where encryption is required as an information safeguard based on the information classification level.

The Fleming College ITS Service Desk is available to assist users with all encryption-related questions.

The Chief Technology Officer has issued this User Standard under the authority of College Policy 6-604 Electronic Information Security Policy.

2 – Encryption versus Password Protection

Password protecting, (a device or file), merely creates a barrier that can be easily bypassed by a technically knowledgeable individual. By contrast, encrypting a device or file protects the information by “scrambling” it to make it unreadable. It is virtually impossible to bypass encryption that complies with the strong encryption standards described below.

3 – Encryption Password/Key Requirements

Strong passphrases or passwords must be used for encryption in compliance with the College’s Password and Passphrase Protection Standard (US-101).

If the encryption password (also called a “key”) is forgotten or lost, the encrypted data is unrecoverable. Therefore, it is essential to have a key recovery plan. A backup copy of the

encryption key should also be securely stored. Users should use a Password Manager, (also known as a Password Vault), to safely store encryption passwords/keys, in addition to traditional access passwords. See the Password and Passphrase Protection Standard (US-101), section 11 – Password Manager Applications, for Fleming supported and licensed password tools.

Fleming College's minimum encryption standard is Advanced Encryption Standard (AES) 256-bit encryption.

4 – File-Level Encryption Requirements

File-level encryption encrypts a single or group of files on a local disk or file system.

The following tools are recommended for file-level encryption:

Product	Version	Operating System (OS) Availability	Software Source & Encryption Instructions
7-Zip	19.00 or newer	Windows Linux	https://www.7-zip.org/ Encrypt files using 7-Zip | Information Technology Services (flemingcollege.ca)
AES Crypt	3.09 or newer	Windows macOS Linux	https://www.aescrypt.com/ AES Encryption Using Windows 10 | Information Technology Services (flemingcollege.ca) AES Encryption using Apple macOS | Information Technology Services (flemingcollege.ca)
Microsoft Office (Word, Excel, PowerPoint)	365	Windows macOS	Downloading and Installing the Microsoft Office 365 Desktop Application | Information Technology Services (flemingcollege.ca) Encrypt Files Using Microsoft Office | Information Technology Services (flemingcollege.ca)
Adobe Acrobat Pro DC (PDF)	2019 or newer	Windows macOS	Adobe Creative Cloud (CC) | Information Technology Services (flemingcollege.ca) Encrypt a file with Adobe Acrobat | Information Technology Services (flemingcollege.ca)

When encrypted files are shared with other users, a password or passphrase will need to be provided to the recipient to open the file. The password/passphrase should be provided to the recipient via a secure communication method, and one that differs from the method used to send/transmit the encrypted content if data transmission/exchange is applicable. For more information on encrypting files for sending/transmission over email or other means, refer to the ITS Standard Transmission and Sharing of Electronic Information (US-103)

If the individual is receiving encrypted files regularly, it is acceptable to use the same password/passphrase for all of these files, as long as it is changed at least once per year.

Also, zipping files does not automatically encrypt them; a zip file is simply a way to compress data into an easy-to-transport package. Most zip programs contain the ability to protect the compressed file with strong encryption, but this feature is not turned on by default. Zipping alone will not keep your information safe.

5 – Device Level Encryption

Device-level encryption requirements apply to Fleming-owned asset devices that are used to access or store Fleming information as per the table below:

Device Type (location and/or context)	Encryption Requirements	Recommended Toolset	End-User Action
Laptop computer	Full disk encryption is required.	Use native encryption for Windows (BitLocker) or macOS (FileVault).	None, Fleming IT assets are provided to end-users with this setting enabled.
Smartphone, tablet, PDA	Device-level encryption is required.	iOS and Android Devices with a vendor-supported OS (still receiving updates) should use native OS encryption.	None, Fleming IT assets are provided to end-users with this setting enabled.
Removable Media (to be avoided where possible for College data, see section 5.1 below)	Device/media-level encryption is required.	Use OS native encryption for Windows (BitLocker to Go) or macOS (FileVault). Or media device with a physical encryption module that is FIPS 140-S compliant may also be used.	Users should contact the IT Service Desk for assistance with configuring software encryption or purchasing a hardware-enabled device.
Desktop Computers (Domain Joined)	Full disk encryption is not required. Domain joined PCs are configured not to save user data to the local hard drive.	NA	NA
Desktop Computers (Not Domain Joined)	Full disk encryption is required.	Use native encryption for Windows (BitLocker) or macOS (FileVault).	None, Fleming IT assets are provided to end-users with this setting enabled.
Servers, located in the	No full disk encryption is required.	NA	NA

Fleming ITS Datacentre			
Storage area network (SAN), located in the Fleming ITS Datacentre	No full disk encryption is required.	NA	NA

Even in situations where encryption is not required above, it may be required to meet additional obligations such as legal or contractual requirements.

If a college device is lost or stolen, the College needs to be able to accurately report its encryption status. College asset devices must adhere to this standard and no person should remove or circumvent any device level encryption that is configured or enabled by manufactured default unless explicitly authorized to do so by Fleming's Chief Technology Officer.

All lost or stolen asset devices must be reported to the ITS Service Desk.

5.1 – Removable Media

Storing sensitive information on portable/removable media should be avoided where possible and only when a defined legitimate business need to do so exists. If the use of removable media is necessary, device/media-level encryption is required as stated in the table above.

Due to the elevated risk of loss, theft, and inappropriate disclosure, the following safeguards must be implemented to secure removable media when not in use:

- Physical removable media must be stored in a secure & locked location, such as a room accessible only by staff with a key or access card.
- Physical removable media must be stored in a secure & locked container, such as a safe, file cabinet, or lockable desk drawer.

6 – Cloud-based Encryption Requirements

Encryption requirements apply to Fleming College data, applications, and information systems stored and accessed using cloud-based technologies. Encryption must be implemented as follows:

Service Types	Encryption Requirements	Recommended Toolset
Virtual servers (e.g. Amazon Web Services, Microsoft Azure, etc)	Full disk/volume encryption is required.	Use native encryption for Windows (BitLocker) or Linux (LUKS with a key size of 256-bits or more) or service-specific (using AES-256 algorithm or better)
Object-based or other cloud storage services	Full volume encryption is required.	Service-specific (using AES-256 algorithm or better)
Software-as-a-Service (SaaS)	Applications containing Confidential or Highly	All cloud vendors must be approved by the ITS Department and have

Platform-as-a-Service (PaaS)	Confidential information must use encryption. Application containing Public and Internal only information should be encrypted where possible.	undergone the Higher Education Community Vendor Assessment Toolkit (HECVAT) review process.

Even in situations where encryption is not required above, it may be required to meet additional obligations such as legal or contractual requirements.

7 – Related Documents

- College Policy - Electronic Information Security Policy (6-604)
  - College Procedure: Information Security Classification Operating Procedure (OP 6-604A)

- IT Standard - Password and Passphrase Protection (US-101)
- IT Standard - Transmission and Sharing of Electronic Information (US-103)

- Information Sensitivity Labels | Information Technology Services (flemingcollege.ca)
- 1Password – Password Manager/Vault | Information Technology Services (flemingcollege.ca)

- Advanced Encryption Standard (AES) | NIST
- FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov)

- Educause - Higher Education Community Vendor Assessment Toolkit (HEVCAT) https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

8 – History of Amendments & Reviews

N/A