Procedure Title:	Access Control Procedure
Procedure ID:	6-604B
Manual Classification:	Section 6 – Information Technology
Linked to Policy:	6-604 Electronic Information Security Policy
Approved by Senior Management Team:	2022-03-30
Revision Date(s):	2022-03-30
Effective Date:	2022-07-01
Next Review Date:	2025-06-01
Contacts for Procedure Interpretation:	CTO Directors, Information Technology

1.0 – Purpose

Information is a valuable asset and access to it must be managed with care to ensure that confidentiality, integrity, and availability are maintained.

This procedure outlines the rules relating to authorizing, monitoring, and controlling access to Fleming accounts, information and information systems.

2.0 – Definitions and Acronyms

The following definitions and/or acronyms apply in this Procedure:

All Users	The set of all individuals who use Fleming College IT systems or resources, usually via a designated user account.
Application or System Administrator	Any user who manages the upkeep, operation, and configuration of an electronic system or application. These users can be identified by having administrative privileges over the system or application.
Data Custodians	An employee of the College with any level of operational authority, responsibility, expertise, and knowledge about a data source, application, or storage in their functional area. Data Custodians are responsible for data creation, collection, classification, labeling, safeguarding, provisioning access, copying, moving, and disposing of data, at an operational level in their functional area in compliance with this procedure.
Data Stewards	Any administrative employee of the College that ensures individuals that have access to sensitive information are aware of their responsibilities to protect that information as described in this procedure.

Data Trustee	A senior administrative employee that has responsibility for a functional area of the College and any records related to that function. The Data Trustee is accountable for ensuring that its records are maintained according to this procedure. (See related definition of Office of Primary Interest.)
Office of Primary Interest	In alignment with the Canadian Library and Archives, the OPI is the office or department that has the main responsibility for a subject area and any related records. The OPI, as the primary Data Trustee, is accountable for ensuring that its records are maintained according to College Policy, Operating Procedures, and Standards. For example, the department responsible for the recording of minutes by a committee would be considered the OPI and must ensure that those records are properly classified and protected.

3.0 – Scope

This procedure applies to any person or systems that are granted or that grant access to accounts, information, or information systems owned or operated by Fleming College.

4.0 – General Principles

Compliance with this operating procedure enables consistent controls to be applied throughout the College, minimizing exposure to security breaches, whilst allowing systems and security administration and technical support staff to conduct their activities within applicable legislative and/or contractual obligations.

Access to information assets, accounts, systems, and resources based on the principle of least privilege.

This procedure aims to ensure that, by having the appropriate access controls in place, the right information is accessible by the right people at the right time and that access to information, in all forms, is appropriately managed and periodically audited.

4.1 – Responsibilities

All Users at Fleming must abide by the Colleges' relevant Electronic Information Security Policy, Information Security Classification Procedure, and this Access Control procedure.

All Users must:

- Only use their account and access in accordance with the Electronic Information Security Policy and the Appropriate Use Policy.
- Secure their credentials in line with the Fleming ITS Standard for Password and Passphrase Protection.
- Be responsible for systems, services, and data within their control.
- Transfer services for data before vacating a role or leaving the College.

All supervisors must:

- Only sponsor access requests for their employees that have:
  - A documented request
  - Adequate and appropriate justification, based on the employee's business need
- Document all access request sponsorships

Data Trustees, Data Stewards, and Data Custodians must:

- Periodically review access to their assets and investigate any anomalies. Review periods are based on the risk and sensitivity rating of a given asset.

System and Application Administrators must:

- Only grant access requests that have:
  - A documented request
  - Adequate and appropriate justification, as confirmed by the supervisor
  - Documented sponsorship by the supervisor
  - Subsequent authorizing approval from the Data Trustee or Data Steward
- Document all access grants

5.0 – Access Control

5.1 – Access Control Requirements

The Access Control Requirements Table shown in Appendix A itemizes several security safeguards that are either required, recommended, or optional, based on a system's or asset's information classification level.

5.2 – Access Governance Principles

A formal user access provisioning process is implemented to assign or revoke access rights for all user types to systems and information assets under the control of the College.

This access provisioning is based on the following principles:

Access changes for employees are primarily managed through the ITS Service Management / Ticketing system.

- All extra requests for or changes to access are documented and tracked.
- All access requests or changes require documented justification.
- Justification will be based on a simple risk assessment and the business need and will be confirmed by the request sponsor.
- Appropriate sponsorship & approval is required and documented for all access requests or changes.
- All access changes granted by administrators are documented and tracked.
- Reviews of access are performed by relevant asset owners periodically.
- These principles are agnostic of account type, service, application, or system.

5.2 – Access Requests

The following steps are used to facilitate access requests. Each step will be primarily managed and documented through the ITS Service Management / Ticketing system.

a) **Request** – Upon identification of a user needing access to College information, a written request will be documented. For employees, contractors, and student workers, the

request must be sponsored by a supervisor with justification of the business need, e.g. information necessary to perform a job function.

b) **Approval** – Authorization to grant access must come from the Data Trustee or Data Steward who has responsibility and authority for the record, information, or system access being requested. Requests are to be appropriately considered and may be approved, denied, or seek further information regarding the request.

c) **Grant** – After authorized approval has been granted, a System or Application Administrator will proceed to implement the technical access provision within the system or application.

5.3 – Employee Offboarding Removal or Adjustment of Access Rights

The access rights of all employees to information and information processing facilities will be removed upon termination of their employment, contract, or agreement, or adjusted upon change.

It is the responsibility of the employee's supervisor to inform ITS of staff leaving their employ. The IT Service Request can be submitted by the employee's supervisor, the division's Administrative Assistant, or HR Consultant.

The ITS Department will maintain a checklist of all College systems and assets for offboarding or role change purposes.

System and/or Application Administrators will proceed to remove the employee's access rights.

Additional access to accounts, assets, systems, or services are subject to review and approval on a case-by-case basis.

5.4 – Access Reviews

Access to assets, services, and systems will be periodically reviewed. The frequency of these reviews depends on the identified risk and information sensitivity surrounding the asset and access in question.

Information Classification Level	Access Review Frequency
Highly Confidential	Minimum annually, once a semester recommended.
Confidential	Minimum annually. Anytime there is a significant change to roles and/or personnel.
Internal	Minimum every two years, annually recommended.
Public	Every two years recommended, or as directed by the OPI.

Access reviews must also be performed anytime there is a significant change to roles and/or personnel within the scope of existing access rights.

The risk and sensitivity relating to each individual asset is measured and given a risk rating in-line with Information Classification Levels described within OP #6-604A Information Security Classification Procedure.

Where an access review identifies an access anomaly it will be treated as a potential incident and investigated by the Office of Primary Interest (OPI) and IT information security team as described by OP #6-604C Information Security Incident Management.

6.0 – Related Documents

- PIPEDA – *Personal Information Protection and Electronic Documents Act* (2000)
- FIPPA - *Freedom of Information and Protection of Privacy Act* R.S.O. 1990 c. F. 31
- PHIPA – *Personal Health Information Protection Act* (2004)
- College Policy #1-108, Enterprise Risk Management
- College Policy #1-111, Access to Information and Protection of Privacy
- College Policy #1-112, Information Practices Related to Personal Health Information
- College Policy #6-601, IT Appropriate Use Policy
- College Policy #6-604, Electronic Information Security Policy
- OP #6-604A, Information Security Classification Procedure
- OP #6-604C, Information Security Incident Management
- Fleming ITS Standard: Password and Passphrase Protection
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171 Rev.2)
- International Organization for Standardization, Information security management systems – Requirements - ISO 27001

History of Amendments & Reviews

N/A

Appendix A – Access Control Requirements Table

Access Control ID	Control Description	Information Security Classification				Access Control Framework Reference
		Public	Internal	Confidential	Highly Confidential	
AC-1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Required	Required	Required	Required	ISO 27001) A 9.2.2 NIST 800-171) 3.1.1
AC-2	Limit system access to the types of transactions and functions.	Recommended	Recommended	Required	Required	ISO 27001) A 9.4.1 NIST 800-171) 3.1.2
AC-3	Control the flow of the College's data in accordance with approved authorizations	Recommended	Required	Required	Required	NIST 800-171) 3.1.3
AC-5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Recommended	Recommended	Required	Required	ISO 27001) A 9.4.1 NIST 800-171) 3.1.5
AC-6	Use non-privileged accounts or roles when accessing non-security functions.	Recommended	Recommended	Required	Required	ISO 27001) A 9.4.4 NIST 800-171) 3.1.6
AC-7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit	Required	Required	Required	Required	ISO 27001) A 9.2.3 NIST 800-171) 3.1.7

Appendix A – Access Control Requirements Table

Access Control ID	Control Description	Information Security Classification				Access Control Framework Reference
	logs.					
AC-8	Limit unsuccessful logon attempts.	Recommended	Required	Required	Required	ISO 27001) A 9.4.2 NIST 800-171) 3.1.8
AC-9	Provide privacy and security notices consistent with applicable College policies.	Required	Required	Required	Required	NIST 800-171) 3.1.9
AC-11	Terminate (automatically) a user session after a defined condition.	Optional	Recommended	Required	Required	NIST 800-171) 3.1.11
AC-12	Monitor and control remote access sessions.	Recommended	Required	Required	Required	NIST 800-171) 3.1.12
AC-13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Recommended	Required	Required	Required	ISO 27001) A 10.1.1 NIST 800-171) 3.1.13
AC-14	Route remote access via managed access control points	Recommended	Required	Required	Required	NIST 800-171) 3.1.14