Procedure Title:	Information Security Classification Procedure
Procedure ID:	6-604A
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

Fleming College collects, creates, and maintains information resources to operate the College and is required to handle that information responsibly through controls and data governance practices. This procedure provides direction on handling electronic information with direction on creating, collecting, classifying, labelling, securing, storing, using, copying, transferring, and disposing of information.

The purpose of this procedure is to set out the minimum standards necessary for classifying various types of college information resources so that reasonable security protections can be applied to such information.

2.0 – Definitions and Acronyms

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

Application or System Administrator	A 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.
College Community	All people who study, teach, conduct research at or works at, or under, the auspices of the College and includes without limitation: employees, contractors; appointees (including volunteer board members); students; visitors; and any other person while they are acting on behalf of, or at the request of the College.
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 policy.

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 policy.
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 policy. (See related definition of Office of Primary Interest).
ISMS	An Information Security Management System is a systemic approach to managing sensitive organization information so that it remains secure. It is comprised of people, processes, and technologies that manage the overall security of the organization's systems and data.
IT Standards	IT Standards are specific and granular requirements that give direction to support broader level IT policies.
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.
Removable Media	Refers to data storage devices for computer systems that can be removed without powering off the system and are portable. Examples include but are not limited to USB/flash drives, CDs, DVDs, and magnetic tapes.

3.0 – Scope

This policy applies to all members of the College Community that use any Fleming College information regardless of their role, location, device, or facility.

This procedure must be interpreted and applied in compliance with the College's obligations under all collective agreements. Nothing in this Policy must be interpreted as limiting or amending the provisions of any collective agreement. To the extent that this Policy may conflict with the College's obligations under any collective agreement, the collective agreement prevails provided that its provisions do not conflict with FIPPA or PHIPA.

4.0 – General Principles

4.1 – Personal Information

College Policy, Operating Procedures, Standards, and processes, for the collection and management of personal information, are defined based on and are subordinate to, Personal Information Protection and Electronic Documents Act (PIPEDA), the Freedom of Information and Protection of Privacy Act ("FIPPA") and College Policy 1-111 Access to Information and Protection of Privacy.

4.2 – Health Information

College Policy, Operating Procedures, Standards, and processes, for the collection and management of health information, are defined based on and are subordinate to, the Personal Health Information Protection Act, 2004 ("PHIPA") and College Policy 1-112 Information Practices Related to Personal Health Information.

4.3 – Classification of Information

Information resources must be assigned a security classification level in accordance with the classification levels below and further described in Appendix A.

Sensitivity	Colour	Classification Level
Sensitive	Red	Highly Confidential
Sensitive	Red	Confidential
Sensitive	Yellow	Internal
Non-Sensitive	Green	Public

Awareness: Before assigning a security classification level the Data Trustee and Data Steward must be aware of relevant legislative requirements, regulatory obligations, and relevant college policies and procedures.

Classify: The Data Trustee and/or Data Steward acts as the administrative authority to assign a security classification level for resources for which they are accountable and responsible.

As required, the Data Trustee and/or Data Steward will consult with the College's CTO and Privacy Officer to classify the information resources for which they are responsible.

Where multiple subsets of information are stored together, that information is classified at the highest level of sensitivity in the subset. (The classification of information may change over time. For example, a draft or working document may be classified as Internal until the final version is published as Public.)

The Data Trustee and/or Data Steward will inform the Data Governance Committee of any additions or changes needed to the Inventory of Records.

4.4 – Labelling of Information

To support consistent information handling practices, information classified as Confidential and Highly Confidential must be labelled with their information classification. This includes but is not limited to electronic labels, tags, and watermarks, where supported and feasible.

Information classified as Internal, or Public may be labelled at the discretion of the author.

4.5 – Safeguarding of Sensitive Information

The ITS Director of Infrastructure is responsible for the implementation of security safeguards on the Fleming network and infrastructure and College asset end-user computing devices.

The ITS Director of Applications & Information Management is responsible for the implementation of security safeguards for enterprise applications and information resources.

The ITS Director of Security is responsible for the implementation of the ISMS and oversight of related controls.

Data Trustees are required to ensure that appropriate safeguards are put in place which includes technical, physical, and administrative safeguards as necessary.

Sensitive electronic information must be stored on authorized College systems. Authorized College systems must be approved by the Data Trustee and CTO for a specific purpose, with a defined scope of use, and for storing specific types of sensitive information. The Data Trustee or CTO will inform the Data Governance Committee of systems approved for the storage of sensitive College information so that the Inventory of Records can be updated accordingly. Changes to the system's scope of use or data storage requirements for sensitive data will require the system to be reauthorized.

System and/or Application Administrators must configure systems that safeguard sensitive information in compliance with the College's IT Standards.

Storing sensitive information on removable media should be avoided where possible and used only where a defined legitimate business need to do so exists. Strong encryption must be used to protect information stored on any removable media in compliance with the College's ITS Encryption Requirements.

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

- Physical removable media must be stored in a secure and 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 and locked container, such as a safe, file cabinet, or lockable desk drawer.

4.6 – Providing Access to Sensitive Information

Access to sensitive information must be authorized on a need-to-know basis and be based on job role. Users must request access to information and authorization must be performed by a Data Trustee or Steward. Electronic access is provisioned by an Application or System Administrator once authorized.

Refer to OP #6-604B Access Control Procedure for further information on access controls.

4.7 – Copying or Moving Sensitive Information

Any action to copy, move, duplicate, or relocate sensitive information without approval from the originating Data Trustee is prohibited. If approved, the Data Trustees overseeing the relocation are responsible for complying with all provisions of this policy.

4.8 – Creating and Maintaining High Quality Information

Information must be collected, created, modified, and maintained with assurance that the information quality and integrity are accurate, complete, and consistent with business requirements such that it can be used for its intended purpose and reporting requirements. Information identified to be of low quality must be corrected at its source and replicated to downstream systems where appropriate. Departments must maintain business documentation such as training materials, standards, controls, information flows, and retention schedules for information under their stewardship.

4.9 –Transfer of Sensitive Information to Third Parties

Transferring sensitive information outside of the College must comply with Fleming College's privacy and legal statements, and, where that information includes Personal Information, that transfer must be consistent with legislative requirements. Data Trustees should consult with the Privacy Officer and the CTO (or designate) for guidance as appropriate.

Strong encryption must be used to protect information in transit in compliance with the College's IT Standards for Encryption, and Transmission and Sharing of Electronic Information.

Electronic transfer of non-encrypted and personally identifiable information outside of the College via end-user technologies (i.e., e-mail, instant messaging, or SMS text message) is strictly forbidden when the transfer is not performed directly to the information subject.

Transportation of Personal Information using removable media to other organizations, or third parties should be avoided where possible. If required, device encryption and a chain of custody log must be created, stored, maintained, and updated.

4.10 – Record Retention and Disposition

Each functional unit of Fleming College led by a Data Trustee will determine the types and categories of records for which they are responsible, making them the OPI for those records.

The OPI will document the retention and disposition, requirements, and schedules, for all records for which they are responsible. The OPI will provide this information to the Data Governance Committee for inclusion in the Inventory of Records.

The retention and disposition schedule developed by the OPI shall be in accordance with business and legal requirements, any relevant provincial or federal statutes, contractual agreements, and any other applicable standards.

The retention and disposition schedules are determined based on the needs for each functional unit within Fleming College. The potential value of records should be evaluated against the cost of storage when establishing records retention periods by avoiding exaggeration of the frequency of reference to records.

Determining the disposition will establish whether the records will be disposed of, archived, or treated with some special consideration. A records retention and disposition schedule includes:

- The period of time for which records are considered active and kept on a computer or in office space.
- The point at which records become semi-active (dormant) and are transferred to storage or offline media.
- The total periods of time for which the records are maintained in storage.
- Disposition of records or permanent preservation.

Disposition of College records must ensure that no sensitive information is exposed.

Staff leaving the College or who relinquish their position must leave all College records.

4.11 – Disposal of Sensitive Information

Electronic media containing sensitive information must be delivered to the IT Service Desk for secure disposal or reuse in compliance with IT Standards.

When a department disposes of personal information records, a data disposal log must be filled out and retained by the destroying department. This requirement does not apply to transient customer service transactions such as an individual registration form or letter.

4.12 – Accidental Loss or Inappropriate Disclosure of Sensitive Information

Loss or disclosure of sensitive information must immediately be reported to the Data Trustee and CTO (or designate). Loss or disclosure of sensitive information that contains Personal Information must immediately College's Privacy Officer.

4.13 – Awareness and Right to Audit

Upon request of the CIO, Data Trustees must perform access audits to ensure that only the correct and authorized users have access to sensitive information under their control. The CIO, Internal Audit, Legal, Privacy, and IT Security staff among others, acting on behalf of the College may conduct information governance, security, or privacy audits at any time to validate controls against this policy and any laws, regulations, policies, standards, and procedures.

5.0 – 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 #6-600, IT Policy Framework
- College Policy #6-601, IT Appropriate Use Policy
- College Policy #6-604, Electronic Information Security Policy
- College Policy #9-904, Intellectual Property and Copyright
- OP #6-604B Access Control Procedure
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-88 Rev. 1, Guidelines for Media Sanitization (NIST SP 800-88 Rev.2)

History of Amendments & Reviews

N/A

Appendix A – Information Classification Levels
College information resources are classified according to the classification levels in the following chart.

Sensitivity	Public	Internal	Confidential	Highly Confidential
Definition	Information that has been approved for distribution to the public by the OPI, administrative authority or through some other valid authority such as legislation or policy.	Information that is intended for use within the College or within a specific department, school, committee, workgroup or any group of individuals with a legitimate need-to-know. Internal information is not approved for general circulation outside the group.	Information is highly sensitive business or Personal Information, or a critical system. It is intended for very specific use and may not be disclosed except to those who have explicit authorization to review such information, even within a workgroup.	Information is so sensitive or critical that it is entitled to extraordinary protections, as defined in Appendix B.
Legal Requirement	Information may be mandated by legislation (e.g. FIPPA) to be public information.	The College has a contractual obligation to protect the information.	The College has a contractual or legal obligation to protect the information.	Protection of information where it is required by law (e.g. FIPPA) or regulation, or as determined by a contractual obligation.
Risk *(Of loss)* *Reputational* *Operational* *Financial* *Disclosure*	**Low** • No impact to reputation. • Little or no impact on ability for business unit to achieve its objectives. • Impact is within normal operating budget. • Disclosure of public information requires no further authorization and may be freely disseminated without potential harm to the College.	**Medium** • Potential for loss of trust/creditability. May generate some media attention and result in increased scrutiny. • Moderately impacts business unit's ability to achieve its objectives. • Minor negative financial impact for business unit. • Possible adverse impact on College or individuals.	**High** • Significant loss of trust/credibility. Will generate media attention and increased scrutiny. • Significant impact on business unit's ability to achieve its objectives. • Significant revenue loss, or impact to budget, including research funding, or fines. • Moderately adverse negative impact on College or individuals, including the potential for identify theft.	**Very High** • Significant loss of trust/credibility. Will generate media attention and increased scrutiny. • Significant impact on business unit's ability to achieve its objectives. • Significant revenue loss, or impact to budget, including research funding, or fines. • Moderately adverse negative impact on College or individuals, including the potential for identify theft.

Appendix B – Security Protections for Information Classification Levels

After an information classification has been applied, reasonable security arrangements are required that correspond to the assigned classification level. The following table set out appropriate minimum safeguards for each level of information.

	Public	Internal	Confidential	Highly Confidential
Access	No access restrictions.	• Access is limited to employees and other authorized Users for business related purposes. • Access must be revoked as soon as reasonably possible when Users leave the College or OPI.	• Access is limited to individuals in a specific function, group, or role. • Principles of least-privilege and need-to-know must be applied. • Access must be revoked as soon as reasonably possible when Users leave the College or OPI.	• Access is limited to specific named individuals or positions. • Principles of least-privilege and need-to-know must be applied. • Access must be revoked immediately when Users leave the College or OPI.
Digital Transmission (e.g. WiFi, email, https, etc.)	No special handling required.	• Encryption for public network (e.g. wireless, Internet)	• Encryption for public network (e.g. wireless, Internet). • Encryption for trusted and internal networks. • External email to be avoided where possible. If required, use of email encryption is recommended. • Internal email must be labelled "confidential".	• Encryption for public network (e.g. wireless, Internet). • Encryption for trusted and internal networks. • External email strongly discouraged in all cases. If absolutely required, must use email encryption. • Internal email must be labelled "confidential" (at a minimum) or "highly confidential" and strongly recommend the use of email encryption.
Physical Mailings	No special handling required.	• Via inter-office mail or regular postal mail using a sealed envelope.	• Via inter-office or postal mail, in both cases must use a sealed envelope clearly labelled "confidential".	• Via inter-office or regular postal use strongly discouraged. • Hand delivered internally.

				• Trackable courier or registered mail only as required. Must double enveloped, be clearly marked as “confidential” on inner envelope and physical documents.
Storage	• Stored within a system the ensure that only authorized personnel can alter the information.	• Stored within a secure and controlled-access system E.g. password protected file or file system, limited access physical area, or locked file cabinet, etc. • Encryption recommended. • Strongly discouraged on removable or portable media. If required, must be encrypted.	• Stored within a secure and controlled-access system E.g. password protected file or file system with multi-factor authentication (MFA) recommended, limited access physical area to OPI staff only or others while monitored/escorted, or locked file cabinet, etc. Implement “clean desk” policy. • Encryption mandatory on mobile devices & laptops and recommended in all environments. • Physical records must be stored in Ontario, Canada. Digital records must be stored in Canada (preferred) or United Stated (with CIO approval), using an industry accredited and ITS approved vendor. • Not permitted on removable or portable media.	• Stored within a secure and highly controlled-access system E.g. password protected file and file system with multi-factor (MFA) authentication strongly recommended, limited access physical area to OPI staff only or others while monitored/escorted, and locked file cabinet, etc. Implement “clean desk” policy. • Encryption mandatory on mobile devices & laptops, and strongly recommended in all environments. • Physical records must be stored in Ontario, Canada. Digital records must be stored in Canada (preferred) or United Stated (with CIO approval), using a vendor approved by ITS. • Not permitted on removable or portable media.
Destruction	Recycle	• Secure shred for physical documents.	• Secure shred for physical documents.	• Secure shred for physical documents.

		• Digital media shall be destroyed in compliance with NIST SP 800-88 media sanitization guidelines. ITS to degauss magnetic media with certified coercivity. ITS to use certified and documented physical destruction service for non-magnetic media. Cryptographic erase for devices using FIPS 140 validated encryption modules.	• Digital media shall be destroyed in compliance with NIST SP 800-88 media sanitization guidelines. ITS to degauss magnetic media with certified coercivity. ITS to use certified and documented physical destruction service for non-magnetic media. Cryptographic erase for devices using FIPS 140 validated encryption modules.	• Digital media shall be destroyed in compliance with NIST SP 800-88 media sanitization guidelines. ITS to degauss magnetic media with certified coercivity. ITS to use certified and documented physical destruction service for non-magnetic media. Cryptographic erase for devices using FIPS 140 validated encryption modules.

Appendix C – Information Classification Examples
The following chart provides examples of the types of information and their required security classification.

Security Classification	Information
Public	Annual reports Advertising and media releases Product and service information Name and work contact information of employees Academic calendar Job postings Name of diploma and certificate recipients Open-session meeting minutes Campus maps Research publication information of a non-personal, non-proprietary nature
Internal	Student number Staff number Fleming network username Fleming email address Budget information Student grades and assessment scores Some department procedures
Confidential	**Personal Information** Any as defined under FIPAA Home/personal address, phone number, cell number, personal email address Personnel Files Personal vehicle information Personal financial information (bank accounts, payment history, financial aid/grants) Payroll information (tax records, employee payroll, etc.) Insurance benefit and benefactor Pension records Student contact or class list Enrolment status of an individual Academic advising and counselling information **Research Information** Granting agency agreements Sensitive research data **Business/Vendor Data** Contract information **Other College Data** Information that could allow somebody to hard the security of individuals, system, or facilities such as physical campus or critical infrastructure details. User account passwords, passphrases, and other authentication credentials.

Highly Confidential	**Personal Information** Social Insurance Number (SIN) Official government identity card (e.g., Passport ID, Driver's License, etc.) Date of Birth (DoB) Full face images and other biometric identifiers Criminal record checks **Personal Health Information (PHI)** Any defined under PHIPA Medical records Disability and medical accommodation information **Other College Data** Legal suits Closed or in camera Board of Governors documents Academic concessions Appeals and grievances Harassment and discrimination reports
Prohibited	Credit Card Data / Payment Card Industry Data Security Standard (PCI DSS) (when taken as part of a financial transaction)