Procedure Title:	Information Security Incident Management
Procedure ID:	6-604C
Manual Classification:	Section 6 – Information Technology
Linked to Policy:	6-604 Electronic Information Security Policy
Approved by Senior Management Team:	2022-10-11
Revision Date(s):	2022-10-04
Effective Date:	2022-10-11
Next Review Date:	2025-10-11
Contacts for Procedure Interpretation:	CTO

1.0 – Purpose

Compromises in information security can potentially occur at every level of computing from an individual's desktop computer to the largest and best-protected systems at the College. Incidents can be accidental or deliberate attempts to break into systems; purpose or consequence can be from benign to malicious. Regardless, each incident requires a careful response, at a level commensurate with its potential to cause harm to an individual and the College.

The purpose of this procedure is to enable an efficient and coordinated response to a security incident, to clarify the roles and responsibilities, and establish a process to investigate, identify the scope of, contain and remediate the information security incident.

This procedure sets out the steps to take when any member of the College Community becomes aware or suspects that an information security incident has occurred. It is important to act immediately, review and if necessary, repeat some of the steps below.

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.
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 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.)
Information Security Incident	Covers every instance of theft, loss, and collection, use, retention, disclosure, or destruction of college information that is not consistent with the defined permitted access to the information, whether intentional or in error. As well as malicious attempts to circumvent information security safeguards and detection of malicious computer code. Some examples of information security incidents include: a) Loss or theft of portable devices b) Misdirected emails c) Cyberattacks, including ransomware attacks d) Deliberate unauthorized access to records under the custody or control of the College, by a member of the College Community or others.
Office of Primary Interest (OPI)	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.
Personal Information (PI)	As defined under FIPPA, personal information means recorded information about an identifiable individual, including: a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual; b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; c) any identifying number, symbol or other particular assigned to the individual; d) the address, telephone number, fingerprints or blood type of the individual; e) the personal opinions or views of the individual except where they relate to another individual; f) correspondence sent to the College by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

g) the views or opinions of another individual about the individual; and,
h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Personal information does not include:

- the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity;
- information about an individual who has been dead for more than thirty years; and,
- records of graduation that are otherwise publicly disclosed.

3.0 – Scope

This procedure applies to all members of the College Community that handle sensitive college information and any person or systems that are granted access to accounts, information, or information systems owned or operated by Fleming College.

Sensitive college information includes any non-Public college record that is classified as either Internal, Confidential, or Highly Confidential, according to the Information Security Classification Procedure (OP #6-604A).

Additionally, the related Privacy Breach Reporting Procedure (Personal Information) (#OP 1-111C) applies to all members of the College Community that handle Personal Information ("PI"). These related procedures are designed to coordinate with each other when a security incident involves personal information and therefore also represents a potential privacy breach.

4.0 – Responsibilities

All Users are responsible for:

a) protecting the integrity of their Fleming user account(s), primarily by maintaining a strong and unique password known only to them. Refer to College's IT Password and Passphrase Protection Standard (#US-101) for more information.

b) immediately reporting any suspected or confirmed information security incidents by following the steps laid out in this procedure.

All Employees are responsible for:

a) ensuring the security and confidentiality of sensitive College information and system access under the custody or control of the College.

b) review, understand, and follow the College policies, procedures, IT Standards, and your department's specific processes, especially those involving the handling of sensitive information.

Data Trustees are responsible for:

a) responding to inquiries from the College Community related to concerns about suspected or confirmed information security incidents related to any College records they have responsibility for;

b) notifying the CTO about suspected or confirmed information security incidents related to any College records they have responsibility for; and

c) ensuring that Data Steward, Data Custodians, and Application or System Administrators under their employ are aware of their information security and access control responsibilities, including this procedure.

ITS Directors are responsible for:

a) maintaining records of all confirmed information security incidents;

b) working with Data Trustees to assist with responses to internal information security inquiries and concerns; and

c) coordinating the effort to respond to information security incidents and mitigating against future information security incidents and breaches.

The **CTO** is responsible for:

a) escalating severe incidents to the Senior Management Team, the President, and General Counsel as warranted at their discretion;

b) reporting annually to the Senior Management Team and the Board of Governors all confirmed Major and Severe information security incidents. See Appendix A – Information Security Incident Classification.

5.0 – Security Incident Procedures

5.1 – Step 1: Report an Incident

Centralized reporting and control of security incident investigations is necessary to ensure that immediate attention and appropriate resources are applied to control, eliminate, and determine the root cause of events that could potentially disrupt the operation of the college or compromise college data.

1. Users must immediately report all suspected information security incidents as follows:

    a) To the IT Service Desk by emailing itsupport@flemingcollege.ca or phoning 1-866-353-6464 x4111. (For urgent assistance after hours and during the weekend, call 705-749-5530 x1615 to speak to the on-call member of the ITS Leadership Team. This after-hours response is best-effort and triaged by the ITS Leadership Team.)

    b) Where the incident involves **Personal Information (PI)** and is therefore also a

suspected privacy breach, notify your direct supervisor(s) who in turn shall notify the applicable Department Head(s). The Department Head(s) will notify the Privacy Coordinator and/or Officer as per OP #1-111C, Privacy Breach Reporting Procedure (Personal Information). Follow this operating procedure and OP #1-111C in tandem for any incident involving Personal Information (PI).

c) Where the incident involves **physical** security issues on a Fleming Campus also contact Campus Security.

d) The report should include the date of the security incident and a description of the nature and scope of the incident. Be as specific as possible, for example, include the names of any files, folders, email subjects, names of systems or other digital assets, etc.

2. Employees are not to initiate an investigation of information security incidents or breaches unless specifically asked to do so by their Department Head(s) or a member of the ITS Leadership Team.

5.2 – Step 2: Initial Assessment

Co-ordinated by the ITS Director(s), the College's Cybersecurity Analyst and other technical staff as assigned will conduct an initial assessment to determine the severity of the information security incident. The incident's severity will be determined based on factors such as the:

a) sensitivity and criticality of the information or information systems involved;
b) operational impact on the college or a business unit;
c) the magnitude of the service disruption;
d) threat potential;
e) expanse or scope of the incident;
f) impact to the college's reputation; or
g) other adverse impacts on the college, individuals, or third parties.

The severity of an incident may not be initially apparent and so actions may change or be repeated at any point during the response as new information is learned.

An incident's severity will determine the future actions surrounding the incident, including notification requirements or the necessity to assemble a dedicated response team.

- Where the information security incident does or may involve the unauthorized disclosure of Personal Information (PI) the Privacy Officer will be informed as per OP #1-111C.
- Depending on the incident severity the CTO shall involve the rest Senior Management Team, the President, and General Counsel as warranted.
- The President, CTO, and General Counsel will determine if an external legal counsel/breach coach is required and provide direction regarding the handling of legal advice related to the incident, including any reports or records created. General Counsel will facilitate the use of external incident response vendors as required.

5.3 – Step 3: Containment

The ITS Director(s), with the cooperation of the administrative authority and/or provider responsible for the information resource, will take reasonable efforts to contain the incident by, for example:

a) stopping the unauthorized practice;
b) recovering the information or records that were improperly collected, used, disclosed, or disposed of;
c) shutting down affected systems;
d) revoking access;
e) changing computer access codes;
f) blocking network access; or
g) correcting weaknesses in physical security; or
h) performing an authorized search and discovery as necessary for any related digital information or artifacts.

In instances where the incident is significant, and time is of the essence, the ITS Department may implement temporary security measures to mitigate any risks related to the incident until the incident has been addressed. In cases where the action will impair the ability of departments, schools, or a large number of users to fulfill their responsibilities, the approval of the CTO (or designate) is required before implementing the mitigating change. Also, see the Emergency Authority section of the Electronic Information Security Policy (#6-604).

5.4 – Step 4: Eradication

After an information security incident has been contained, the ITS Department, administrative authority, or provider responsible for the information or information systems involved will take action to eliminate the problem or mitigate vulnerabilities that may allow a reoccurrence of the incident and provide timely and regular reporting of their actions to an assigned ITS Director.

5.5 – Step 5: Recovery

After an information security incident has been eradicated, the ITS Department administrative authority or provider responsible for the information or information systems will attempt to fully restore the information systems by, for example:

a) restoring information or information systems from backup;
b) validating that the information is complete and accurate or that an information system is operating correctly; or
c) performing additional monitoring

5.6 – Step 6: Follow-up and Correction

Once action had been taken to mitigate the risks associated with the incident, upon the recommendations of the response team (where formed), the CTO and/or ITS Director(s) will determine whether further investigation of the incident is necessary. Once all investigations are complete, a report of the incident will be provided to the CTO and appropriate administrative authorities, which may include:

a) a summary of the incident;

b) corrective actions that were taken;
c) recommendations made for additional safeguards;
d) follow-up actions required; and
e) lessons learned.

6.0 – Incidents that must be Reported

Users must report the following information security incidents (if there is uncertainty about whether a violation has occurred, users must err on the side of caution and report the incident anyway):

All violations of the College's IT Appropriate Use Policy (#6-601) are incidents that must be reported; examples include but are not limited to:

a) use of Fleming computing facilities to commit illegal acts;

b) unsolicited or spam email originating from Fleming sources;

c) unauthorized access, use, alteration, or destruction of Fleming electronic information or Fleming systems, including but not limited to: software, computing equipment, network equipment, and services;

d) theft of any Fleming electronic information whether it be via electronic means or physical theft of any device containing information;

e) loss or theft of any multi-factor authentication device or token; and

f) detection of any malicious computer code such as a virus, worm, spyware, etc., that may manifest itself as unexplained behaviour on desktops, laptops, or servers such as webpages opening by themselves, new files or folders appearing on the local hard drive, and lockouts of user accounts.

7.0 – Related Documents

- Personal Information Protection and Electronic Documents Act (PIPEDA), *S.C. 2000*
- Freedom of Information and Protection of Privacy Act (FIPPA), *R.S.O. 1990 c. F. 31*
- Personal Health Information Protection Act (PHIPA), *S.O. 2004*
- College Policy - Enterprise Risk Management (#1-108)
- College Policy - Access to Information and Protection of Privacy (#1-111)
- College Operating Procedure #1-111C, Privacy Breach Reporting Procedure (Personal Information)
- College Policy #1-112, Information Practices Related to Personal Health Information
- College Policy #6-601, IT Appropriate Use Policy
- College Operating Procedure #6-601, AUP and accessing another user's data
- College Policy #6-604, Electronic Information Security Policy
- College Operating Procedure #6-604A, Information Security Classification Procedure
- College IT Standard – Password and Passphrase Protection Standard (#US-101)
- Information Technology Services (ITS), OneStop website, Report an Incident page: https://department.flemingcollege.ca/its/report-incident/

History of Amendments & Reviews

N/A

Appendix A – Information Security Incident Classification

The College's Enterprise Risk Management Policy and Operating Procedures contains a risk impact (consequence) table outlined in Appendix I of the ERM procedure. The same 1 – 5 scale and similar metrics will be used for Information Security Incident Classification in terms of financial, operational, user, data sensitivity, health and safety, and reputational impacts.

Rating	Finance	Impacts	Examples*
5 – Severe	< $3.5 M	• Total loss of ability to sustain ongoing IT and/or business operations. • Compromise could have a critical impact on the College's ability to function. • **User Impact:** College-wide services will impact All Users, on-site and remote. • **Data Sensitivity:** May handle or include data that is classified as highly confidential. • **Health & Safety:** Widespread staff/visitor safety at risk • **Operations:** Complete disruption unplanned outages < 2 weeks • **Reputation:** Long-term widespread media coverage, major long-term impact	• Large-scale ransomware attack impacting the College's IT infrastructure. • Improper disclosure or loss of highly confidential information.
4 - Major	< $1 M	• Important but not necessarily critical to the organization. • Essential to specific departments or campuses but not the entire business. • Significantly reduced ability to achieve business strategies and objectives • **User Impact:** College-wide services will impact All Users, on-site or remote. • **Data Sensitivity:** May handle or include data that is classified as confidential. • **Health & Safety:** Some staff/visitor safety at risk • **Operations:** Widespread disruption unplanned outages < 5 days • **Reputation:** Medium-term widespread media coverage, medium-term impact	• Detection of a virus on multiple IT servers. • Improper disclosure or loss of confidential information.
3 - Moderate	~ $500K - $1 M	• Risks that have limited effect on the achievement of business strategies and objectives. • Compromise of any of these assets would have a moderate impact on the College's ability to function. Department/group specific applications for key College functions • **User Impact:** Entire campus, wing, or multiple departments, usually < 100 people. • **Data Sensitivity:** May handle or include data that is classified as internal. • **Health & Safety:** Local staff/visitor safety at risk • **Operations:** Minimal disruption unplanned outages < 1 day • **Reputation:** Medium-term localized media coverage, medium long-term impact	• Detection of a virus on multiple College-owned end-user computing devices or a single IT server. • Compromise of a privileged account for a single system. • Improper disclosure or loss of internal only information. • A large volume of spam emails originating from an internal source.
2 – Minor	~ $100K - $500K	• No material impact on the achievement of business strategy and objectives. • Neither essential nor critical to daily operations. • The compromise of any of these assets may inconvenience a few people but would not be a major business disruption to business processes. Department/group specific applications for auxiliary College functions.	• Compromise of a single user's password that does not have access to any sensitive College information other than their own personal information (PI).

		• **User Impact:** Multiple rooms/classrooms, one department, academic simulators, usually > 100 people • **Health & Safety:** Minimal staff/visitor safety at risk • **Operations:** Local disruption unplanned outage for a couple of hours • **Reputation:** Short-term localized media coverage, short-term impact	• Detection of a virus on a single College-owned end-user computing device. • Loss of a staff laptop with appropriate data storage encryption requirements in place.
1 - Insignificant	> $100K	• Trivial impact • These systems/assets and data are typically only used by a few people or a single individual. • **Operations:** No operational risk • **Reputation:** No media coverage, minimal impact	• Receipt of spam or malicious emails that are appropriate ignored, deleted, or reported. • Compromise of a single user's password that does not have access to any sensitive College or personal information.

* As very brief examples without fully specified context and impacts, these examples should not be taken as limiting or prescriptive.