CHAMPLAIN
REGIONAL COLLEGE

Directive on information security incident reporting and protection against cyberthreats

Champlain
COLLEGE LENNOXVILLE

1958
St.Lawrence
CEGEP CHAMPLAIN

Champlain
COLLEGE SAINT-LAMBERT

Revision History

Version	Date	By	Type	Comments
0.1	2024-08-23	Claude Leduc	Creation	
0.2	2024-09-26	Claude Leduc	Modification	Text proofing
0.3	2024-09-30	Claude Leduc	Modification	Added precision following internal comments
0.4	2024-11-06	Claude Leduc	Modification	Text revision following review by the Director General
1.0	2024-11-08	Claude Leduc	Authorization	Authorized by the Director General

Table of contents

1. Preamble

This directive on information security incident reporting and protection against cyberthreats (the "Directive") is part of the Information Security Management Framework.

Champlain Regional College (the "College") is implementing this Directive to promote certain reflexes among its employees and guide them in the event of an information security incident, including preventive measures against cyberthreats.

2. Purpose

The purpose of the Directive is to inform all individuals and entities, whether regular, occasional or contractual, regardless of their status, who are using the College's information assets, of the steps to be taken in the event of an information security incident.

It also specifies the measures to be taken to counter cyberthreats.

3. Legal and regulatory framework

The Directive is based on the following laws, regulations and standards:

- The Government Directive on Information Security
- Government information security management framework
- *Act to establish a legal framework for information technology* (R.S.Q., chapter C-1.1)
- *Act respecting Access to documents held by public bodies and the Protection of personal information* (LRQ, chapter A-2.1)
- *An Act to modernize legislative provisions respecting the protection of personal information* (RLRQ, 2021, chapter 25)
- Regulation respecting confidentiality incidents (LRQ, chapter A-2.1, r. 3.1)
- *Act respecting the governance and management of the information resources of public bodies and government enterprises* (LRQ, chapter G-1.03)
- Regulation respecting the terms and conditions of application of sections 12.2 to 12.4 of the Act respecting the governance and management of the information resources of public bodies and government enterprises
- Regulation respecting the distribution of information and the protection of personal information (chapter A-2.1, r 2)
- Government Information Security Risk and Incident Management Framework
- Government Information Security Practices
- Requirements of the *Ministère de la Cybersécurité et du Numérique* and the *Centres Opérationnels de Cyberdéfense (COCD)*
- All College Bylaws, Policies, and Regulations

4. Scope

Within the scope of application of the College's Information Security Policy and its related Information Security Management Framework, this Directive applies to all the College's individuals and entities, whether regular, occasional or contractual, regardless of their status, who are using the College's information assets.

5. Definitions

COMSI(s): Stands for Organizational Information Security Coordinator. They are involved in the implementation of measures and provides the necessary support to the CSIO, in particular with regard to information security incident and risk management.

CSIO: Stands for Chief of Organizational Information Security. The CSIO is responsible for the overall management of information security within the College. He/she works closely with government information security stakeholders to ensure that information security requirements are met.

Cyberthreat(s): Perceived, credible, potential and apprehended event, with a non-zero probability, likely to undermine information security.

Incident(s): An event that affects or is likely to affect the availability, integrity, or confidentiality of information or, more generally, the security of information systems, in particular an interruption or degradation of services.

Information asset(s): Any digital information, digital document, information system, documentation, computer equipment, information technology, installation, or set of these elements acquired or created by the College to carry out its mission.

Manager(s): Administrative authority within a department or unit, whether pedagogical or administrative.

The College: Refers to Champlain Regional College of general and vocational educations in its entirety including its Constituent Colleges.

6. What to do in the event of an information security incident

In the event of an information security incident, please follow these guidelines:

- **Report the incident:** contact your local IT Services immediately to report the situation.
- **Gather information:** if possible, gather all relevant information such as date, time, circumstances, and error messages to document the incident.
- **Do not delete data:** avoid deleting items that may serve as evidence or be useful for subsequent analysis.
- **Confidentiality:** only share the incident with those who need to know in order to resolve it.
- **Do not pay a ransom:** if you are asked to pay a ransom, do not do so and contact your local IT Services immediately.
- **Do not shut down your workstation:** it is important not to turn off your workstation as this could result in the loss of evidence used during the analysis.
- **Follow IT recommendations:** follow any recommendations given by the IT staff for an effective incident management process.

7. Cyberthreat prevention

To counter cyberthreats, take the following steps:

- Do not download unauthorized software or utilities. If in doubt, contact your local IT Services.
- Do not connect a USB storage or removable media of unknown origin to a College device.
- Do not click on a hyperlink coming from an unfamiliar source or open suspicious attachments or scan QR codes.
- If you receive a malicious (or what seems potentially malicious) email containing a virus or other alert:
    - do not:
        - take any action,
        - reply, or
        - follow the instructions in the email.
    - Notify your local IT Services and forward them the email if asked.

8. Roles and responsibilities

Effective information security measures require that roles and responsibilities are clearly assigned to the various stakeholders within the College.

8.1. Director General

- Approves this Directive.
- Ensures that employee training and awareness activities are conducted.

8.2. Director of Constituent College

Acts as the constituent college's authority, with regards to information security, in compliance with the authority delegated by the Director General. In turn, the Director of Constituent College ensures compliance with and enforcement of this Directive to their constituent college.

8.3. Chief of Organizational Information Security (CSIO)

- Creates and ensures implementation and revision of this Directive.
- Ensures that awareness and training activities are conducted to support the implementation of the Directive.

8.4. Organizational Information Security Coordinator (COMSI)

- Implements this Directive.
- Carry out awareness and training activities are conducted to support the implementation of the Directive.
- Applies appropriate response measures to any information security threat or incident with a view to ensure the security of the targeted information.

8.5. Local Information Technology Services

- Responsible for the application of this Directive at their location.
- Immediately reports any information security incident to the College's COMSI and/or CSIO.
- Actively collaborates with the COMSI(s) in responding to any reported and detected information security incidents or security threats.

8.6. Managers

- Ensure the implementation and enforcement of information security measures, including this Directive, within their department or service.
- Report any information security-related event or threat to their local IT Services.
- Ensure that this Directive is communicated to all employees, partners and contractors within, or associated with, their department and/or service.

8.7. College personnel & students

- Immediately notify local IT Services of any information security incident (hacking or intrusion into a computer system, identity theft, use of computer viruses, etc.) of which they are aware.
- Participate in any action taken to identify or mitigate an information security threat or incident.
- Comply with preventive measures against cyberthreats.

9. Dissemination and update of this Directive

The Chief of Organizational Information Security (CSIO) is responsible for updating this Directive.

The Senior Management Committee (SMC), in conjunction with the CSIO, is responsible for the dissemination of this Directive.

This Directive will be evaluated and revised on a regular basis, particularly with respect to the relevance of its statements to emerging information security issues.

10. Effective date

This Directive comes into effect on the date of its approval by the Director General and remains in force until it is repealed, modified or replaced by another Directive.