CHAMPLAIN
REGIONAL COLLEGE

Information Security Management Framework

Champlain
COLLEGE LENNOXVILLE

1958
St.Lawrence
CEGEP CHAMPLAIN

Champlain
COLLEGE SAINT-LAMBERT

Revision History

Version	Date	By	Type	Comments
0.1	2024-07-11	Claude Leduc	Creation	
0.2	2024-08-20	Claude Leduc	Modification	Added 6.2.4
1.0	2024-09-19	Claude Leduc	Approval	Approved by the Director General

Table of contents

1. Preamble

This framework complements the Information Security Policy[1]. This management framework is derived from the Government Directive on Information Security, which requires public organizations to adopt, implement, maintain and enforce an information security management framework.

It applies to the public bodies under the Act respecting the governance and management of the information resources of public bodies and government enterprises. Its purpose is to strengthen information security governance at Champlain Regional College, hereinafter referred to as the College, by establishing an information security organizational structure and defining roles and responsibilities at all levels of the organization. It also aims to establish a common vision for information security, and to ensure consistency and coordination of efforts in this area.

2. Legal and regulatory framework

The management framework is based primarily on:

- The Government Directive on Information Security
- Government information security management framework
- Key measures: Government cybersecurity policy
- *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
- *Archives Act* (LRQ, chapter A-21.1)
- *Copyright act* (LRC, 1985, C-42)
- Sector-specific laws that govern the mission of each organization.
- The Policy Framework for the Governance and Management of Public Bodies' Information Resources.
- Regulation respecting the distribution of information and the protection of personal information (chapter A-2.1, r 2)
- *Public Service Act* (RLRQ, chapter F-3.1.1)

[1] https://www.crc-sher.qc.ca/college-champlain/governance-documentation/

- Government Information Security Risk and Incident Management Framework
- International standards, including ISO 27000, NIST 800-60 and COBIT
- 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
- Any other applicable laws or regulations.

3. Scope

This framework covers the areas of application that have been adopted in the Information Security Policy.

It also covers all aspects of managing and protecting information, including but not limited to:

- Sensitive or confidential information.
- Strategic or critical information.
- Public information.
- Internal networks, cloud and systems used to backup, process or transmit information.
- Databases and applications used to manage information
- Devices and peripherals (computers, laptops, telephones, printers, scanners, etc.) used to access information.
- Documents and backup media (paper, hard disks, USB sticks, etc.) used to store information.
- Electronic communications (email, instant messaging, etc.) used to transmit or receive information.

4. Definitions

CERT/AQ: Acronym for the Quebec government's information security incident response team and alert network. Computer Emergency Response Team/Administration Québécoise.

Constituent College: Refers to the constituent colleges of Champlain Regional College at which students are registered for educational purposes, namely Champlain - Lennoxville, Champlain St. Lawrence and Champlain Saint-Lambert, individually or collectively according to the context.

Custodian: A manager who is the designated person responsible for the security of an information asset.

Document(s): A set of information carried by a medium. The information is delimited and structured, either tangibly or logically, depending on the medium, and is intelligible in the form of words, sounds, or images. Information may be represented in any form of writing, including a system of symbols transcribed into one of these forms or into another system of symbols. A document includes any database whose structuring elements enable documents to be created by delimiting and structuring the information contained therein.

Incident: 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.

Information technology: Technologies, primarily computer, audiovisual, multimedia, Internet, and telecommunications (wired and wireless networks and telephony), that enable users to communicate, access information sources, store, manipulate, produce, and transmit information.

IT continuity and recovery plan: A set of procedures detailing the steps to be taken to recover a computer system after a failure or major disaster.

Manager: 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 and its Constituent Colleges.

User(s): Any physical or legal person who uses or has access to the College's information resources. This includes, but is not limited to, faculty, professional staff, support staff, managers, students, unions, or associations representing them, student housing tenants, and third-party service providers.

5. Guiding principles

This Information Security Management Framework is implemented to complement the application of the College’s Information Security Policy. The management framework specifies the functional aspects of information security.

Information security practices and solutions are periodically reevaluated to reflect not only legal, organizational, technological, physical, and environmental changes, but also evolving risks and threats.
The College's Information Security Management Framework is based on five guiding principles:

5.1. Identity and access management (IAM)

Identity and access management is monitored and controlled to ensure that access, disclosure, and use of all information held by the College is strictly limited to authorized individuals to protect confidentiality.

5.2. Vulnerability management

Vulnerability management entails taking steps to keep software and hardware in the information technology environment up to date to minimize vulnerabilities and reduce the likelihood of a cyber attack.

5.3. Risk management

Risk management of the College's information assets is based on an analysis of the threats to the integrity, availability and confidentiality of the information held by the College. On a recurring basis, this analysis is used to establish guidelines and directives for the use and operation of information systems and expected outcomes.

Risk analysis also guides the acquisition, development, and operation of information systems, whether local or remote, owned or outsourced, by specifying the security measures to be implemented for their use in the College's environment.

All risks that could affect the government's operations and reputation are reported in accordance with the Government Directive on Information Security.

5.4. Incident management

Incident management is the implementation of procedures for reporting, analyzing, and responding to security incidents. These measures are designed to ensure continuity of service. Incident management allows the College to exercise its authority and prerogatives with respect to any inappropriate use of information assets.

All incidents that could affect government operations and reputation are reported in accordance with the Government Directive on Information Security. (CERT/AQ)

5.5. Business continuity and recovery management

Business Continuity and Recovery Management is characterized by the implementation of processes to identify major operational incidents that could threaten the College, such as natural disasters, power or telecommunications outages, computer failures, hacking, terrorism, pandemics, and so on. Identifying these incidents allows us to assess their impact on the College's activities and to take the necessary mitigation measures to ensure the continuity of critical activities.

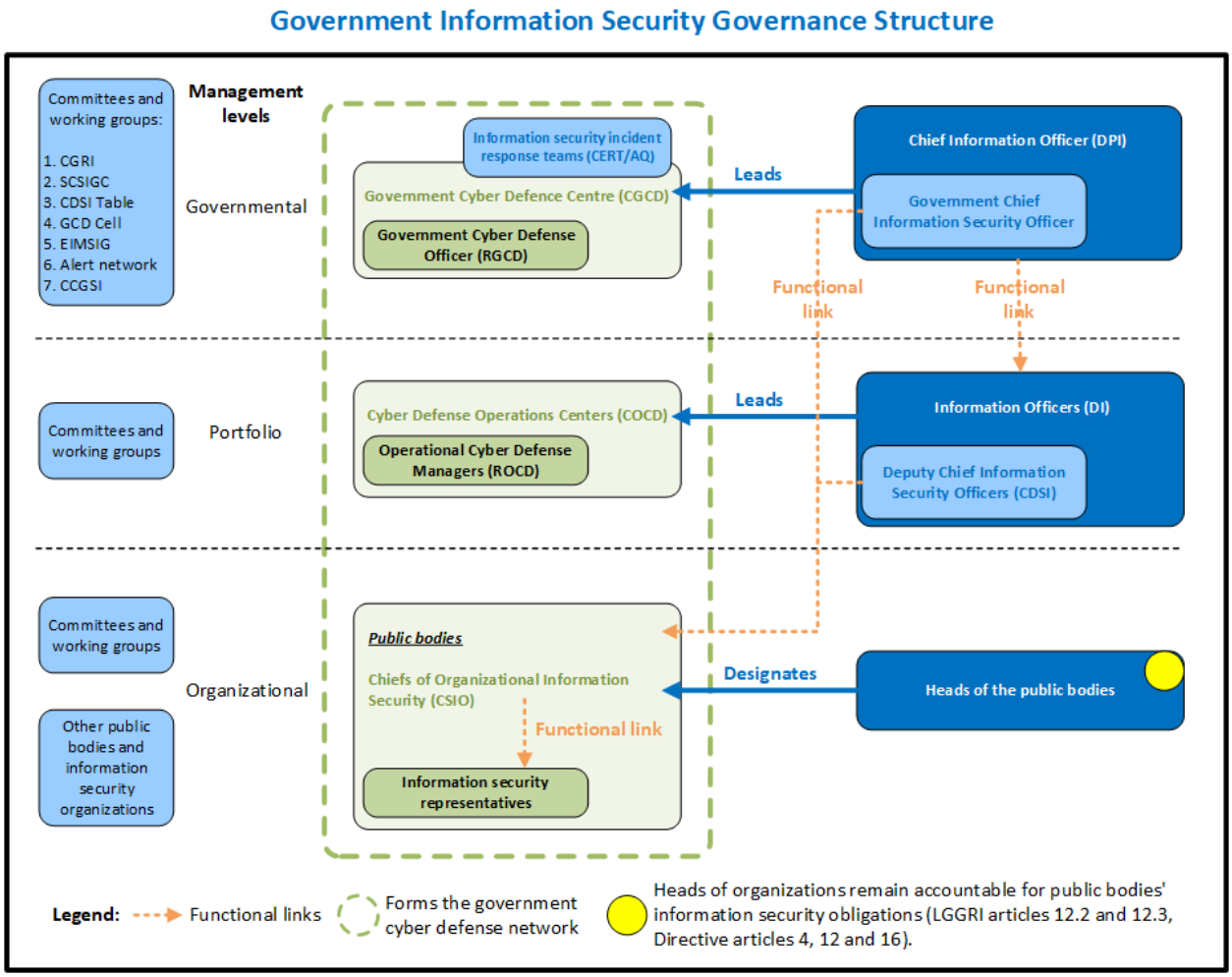
6. FUNCTIONAL ORGANIZATION OF INFORMATION SECURITY

Information security at the College requires an organizational structure that complies with the Government information security management framework. Such a structure must respond to the need to establish strong, integrated sectoral governance that promotes concerted action among stakeholders and enables them to take advantage of the complementarity of their resources and the effectiveness of their actions.

6.1. Government structure

The functional organization of information security within the public administration, in compliance with the Act respecting the governance and management of the information resources of public bodies and government enterprises and the Government Directive on Information Security, is based on a governance structure defined on three management levels, as follows:

- Government level (*Ministère de la cybersécurité et du numérique (MCN)*).
- Portfolio level (Ministry of Higher Education).
- Organizational level (the College).



Source figure 1: Government Information Security Governance Structure (*Cadre gouvernemental de gestion de la sécurité de l'information*, August 2022)

Information Security Officers for specific areas of information security are appointed by the head of their respective public body at the request of the Government Chief Information Security Officer (CGSI), in accordance with Article 11 of the Government Directive on Information Security. Within the functional organization of information security, these officers assume the responsibilities indicated by the Government Chief Information Security Officer (CGSI).

6.2. Functional organization of information security for the College

6.2.1. Director General

The Director General has primary responsibility for the information under their control. They are also responsible for applying the laws that define the legal framework for information management.

As such, they must ensure compliance with the laws and regulations established by the *Conseil du trésor*, particularly with regard to the implementation of measures to reduce the risks to information resources by improving information security. The Director General shall ensure that the various structural elements of information security are implemented, kept up to date and communicated to the Chief Information Officer (DI) of the Ministry of Higher Education. To assist in the performance of their duties, it is preferable for them to acquire qualified personnel at the strategic, tactical and operational levels, or to share existing expertise with other institutions in their network.

These resources will be known respectively as "Chief of Organizational Information Security" (CSIO) and "Organizational Information Security Coordinators" (COMSIs).

6.2.2. Chief of Organizational Information Security (CSIO)

A Chief Information Security Officer (CISO) is responsible for the overall management of information security within the organization. He or she works closely with information security sponsors to ensure that information security requirements are met. Within the information security functional organization, the CISO has the following responsibilities:

- Implement decisions made by the Government Chief Information Security Officer (CGSI) and Deputy Chief Information Security Officer (CDSI).
- Contribute to the implementation of the information security governance framework within the organization.
- Contribute to the implementation of standardized government information security management processes and information security processes developed by the Deputy Chief Information Security Officer (CDSI).
- Ensure that information security requirements are addressed during the development, acquisition, evolution, or replacement of an information asset or information resource service.
- Immediately notify the Deputy Chief Information Security Officer (CDSI) when a security event poses a risk of serious harm.
- Implement the actions required to address an information security event or incident.
- Maintain an information security event registry in accordance with the requirements of the Government Directive on Information Security and the procedures specified by the Deputy Chief Information Security Officer (CDSI).

- Provide the Government Chief Information Security Officer (CGSI) and the Deputy Chief Information Security Officer (CDSI), to whom they report, with the information requested for accountability purposes or as otherwise requested by them.
- Ensures coordination of information security activities undertaken by all stakeholders within the College.
- Establish and coordinate appropriate committees and working groups within the organization to address information security issues.
- Ensure the development of the information security skills of the organization's employees through an ongoing information security training and awareness plan.

6.2.3. Organizational Information Security Coordinators (COMSIs)

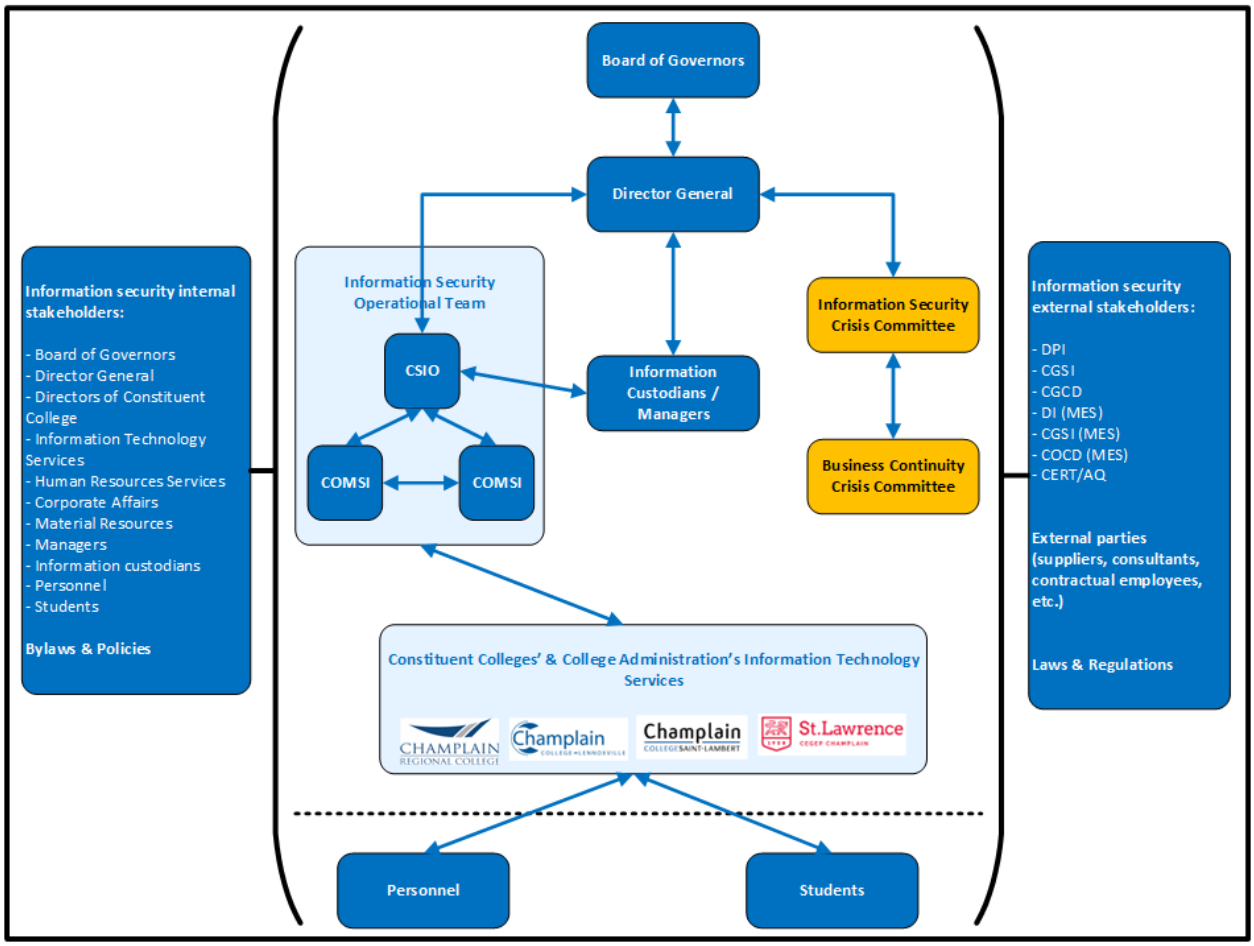
- The COMSI represents the College on the Governmental Alert Network. The COMSI is responsible for implementing the College's Threat, Vulnerability and Incident (GMVI) management process and supporting the Chief of Organizational Information Security (CSIO). In addition to the responsibilities for handling events related to GMVIs, the COMSI must represent the College and actively participate in the Government Alert Network coordinated by CERT/AQC.
- Identify GMVIs affecting the College, notify their CSIO, and escalate as appropriate according to terms defined in the GMVI process.
- Ensure an internal GMVI response plan is developed, updated and implemented.
- Ensure that security risk assessments are performed.
- Work closely with their CSIO and cyber-defense operational manager (ROCD) to provide them with the technical support they need to fulfill their responsibilities.

6.2.4. Information Security Operational Team

- The Information Security Operational Team is an internal team led by the Chief of Organizational Information Security (CSIO) and the two Organizational Information Security Coordinators (COMSIs).
- The main objective of this team is to ensure that the Information Security Policy and this Information Security Management Framework are applied at the organizational level.
- This team is also accountable to their government’s counterparts as defined in 6.1 above. As such, they must also respond to demands, requests, protocols, instructions and directives of their government counterparts.
- This team must also attend weekly information security events. For example, the weekly CERT/AQ meetings, the Cyber Centre Threat Briefing, etc.
- This team is the primary point of contact and collaboration with their internal counterparts at the constituent colleges level.
- Finally, this team is the primary coordinating group in the incident management process.

6.3. Organizational information security structure of the College

Champlain Regional College Organizational Information Security Structure



7. Roles and responsibilities

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

7.1. Director General

The Director General is the primary authority for information security. In this capacity, the Director General ensures compliance with and enforcement of information security laws and regulations, application of the government information security framework, and application of the Information Security Policy and this Information Security Management Framework.

The Director General also approves the Information Security Management Framework.

7.2. Director of Constituent College

The Director of a Constituent College acts as the constituent college's authority, with regards to information security, in conformity with the authority delegated by the Director General. In this delegated capacity, the Director of Constituent College ensures compliance with and enforcement of information security laws and regulations, application of the government information security framework, and application of the Information Security Policy and this Information Security Management Framework to their constituent college.

7.3. Corporate Affairs

Corporate Affairs is responsible for ensuring compliance with and enforcing the law on archives, access to information and the protection of personal information, and for implementing policies and practices governing the protection of personal information.

7.4. Information Technology Services

The Information Technology Services are responsible for the application of the Information Security Policy and this Information Security Management Framework at their location. They ensure that information security requirements are considered in the operation of information systems and infrastructure, and in the implementation of information systems, development, or acquisition projects.

The Information Technology Services assists the CSIO and COMSI in managing, implementing, and reporting on all matters related to information security as defined by government laws, regulations, and frameworks.

7.5. Human Resources Services

In terms of information security, the Human Resources Services must inform all new employees of the College and obtain their commitment to comply with the Information Security Policy and this Information Security Management Framework.

7.6. Material Services

The Material Services, including the various building and equipment services, will work with the CSIO to determine the physical security measures necessary to adequately protect the College's information assets.

7.7. Managers

Managers are the custodians of the information assets in their area of responsibility. Their role is to ensure compliance with applicable rules, frameworks, etc. in ensuring the accessibility, proper use, and security of the information assets under their responsibility.

Managers must also:

- Validate the consistency of profile-based access for each user.
- Ensure the implementation and enforcement of information security measures, including those related to privacy compliance within their department.
- Ensure the security of all information assets entrusted to them in their role as custodians.
- Report any information security-related event or threat to the Information Technology Services.
- Ensure that information security requirements are considered in all procurement processes and service contracts under their responsibility and that all external consultants, suppliers, partners, guests, organizations, and companies agree to comply with the Information Security Policy and all other elements of this Information Security Management Framework.

7.8. College personnel

Responsibility for the security of information rests with all users of the College's information assets. College personnel who access, view, or process information are responsible for its use and must act to protect it.

To this end, the College personnel must:

- Comply with the Information Security Policy and all other College directives and guidelines regarding information security and use of information assets.
- Notify management of any situation that could compromise the security of information assets.
- Use assigned and authorized access rights and the information and systems made available to them only in the context and for the purposes for which they are intended.
- Respect the security measures in place. Do not bypass, modify, or circumvent such measures.
- Immediately notify Information Technology 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.

7.9. Students

The students must:

- Comply with the Information Security Policy and all other College directives and guidelines regarding information security and use of information assets.
- Notify a faculty member or other College personnel of any situation that may compromise the security of an information asset.

- Use assigned and authorized access rights and the information and systems made available to them only in the context and for the purposes for which they are intended.
- Respect the security measures in place. Do not bypass, modify, or circumvent such measures.
- Immediately notify one of the faculty or Information Technology 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.

8. Dissemination and update of the management framework

The Chief of Organizational Information Security (CSIO), in conjunction with the Senior Management Committee (SMC), is responsible for the dissemination and updating of this management framework.

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

9. Effective date

This Information Security Management Framework complements the College's Information Security Policy. It 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 management framework.