CHAMPLAIN
REGIONAL COLLEGE

Information Security Policy

Champlain COLLEGE LENNOXVILLE
1958
St.Lawrence CEGEP CHAMPLAIN
Champlain COLLEGE SAINT-LAMBERT

Adoption and Revision History

Board of Governors Meeting	Resolution Number	Notes
June 14, 2024	CRC-2023-065	

Table of contents

1. Preamble

Champlain Regional College (the "College") recognizes that information and the technologies that support it are essential to its day-to-day operations and to the fulfillment of its teaching and research mission, and that given the administrative, legal and financial value of its information assets, they must be subject to continuous assessment, appropriate and adequate use and protection throughout their life cycle, in accordance with information security best practices and with a risk management approach, regardless of the medium or location.

The application of the Act respecting the governance and management of the information resources of public bodies and government enterprises (R.S.Q., c. G-1.03), the Act to modernize legislative provisions respecting the protection of personal information (R.S.Q., 2021, c. 25), and the Government Directive on Information Security (2021) issued by the *Secrétariat du Conseil du trésor du Québec* and applicable to public bodies, imposes significant obligations on colleges.

In order to comply with its regulatory and legal obligations, the College must adopt, maintain and ensure the application of an information security policy (the "Policy") to ensure the implementation of formal information security processes for risk management, information asset access management, incident management and business continuity management.

2. Purpose

The Policy provides the general framework for managing information assets in accordance with the College's rights and responsibilities on this subject in order to ensure and achieve information security standards and more specifically to:

- Ensure that information assets are protected throughout their lifecycle, regardless of media or location.
- Ensure that information is available when it is needed and can be used by the right people when they need it.
- Ensure the integrity of information by protecting it from unauthorized destruction, modification, or alteration in any way.
- Maintain the confidentiality of information by ensuring that it is not made available or disclosed to unauthorized persons, entities, or processes.
- Consolidate guidelines and the roles and responsibilities of security stakeholders.
- Identify and categorize the College's information assets according to their level of criticality and ensure that they are continually assessed and adequately protected.
- Ensure compliance with applicable laws and regulations.
- Ensure organizational continuity by implementing an IT disaster recovery plan.
- Ensure respect for individual privacy, including the confidentiality of personal information.

3. Legal and regulatory framework

In addition to the College's Information Security Management Framework and related documents, the College must comply with applicable laws, regulations, standards, and government practices.

The Policy exists and is based on these legal and regulatory foundations and is governed by:

- 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
- Rules for managing information resource projects
- Rules regarding the planning and management of information resources
- *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)
- The *Charter of human rights and freedoms* (LRQ, chapter C-12)
- The *Civil Code of Québec* (LQ, 1991, chapter 64)
- The *Criminal Code* (LRC, 1985, chapter C-46)
- *Public Service Act* (RLRQ, chapter F-3.1.1)
- Government Information Security Risk and Incident Management Framework
- Government Information Security 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.

4. Scope

4.1. Targeted audience

The Policy applies without exception to all individuals and entities, whether regular or occasional, regardless of status, who are called upon to use the College's information resources:

- College employees.
- College students.
- College's guests, partners, suppliers, contractors and third parties.

4.2. Targeted assets

The Policy also covers all information and information assets, regardless of the storage, medium (electronic, technological, paper, etc.) that are owned by the College whether:

- It is held by the College itself. Or,
- It is held and/or used by a third party on behalf of the College.

4.3. Targeted activities

The Policy applies to all activities throughout the information life cycle, i.e., the collection, recording, processing, modification, dissemination, retention, and destruction of the College's information assets, whether carried out on the College's premises, at other locations, or remotely.

5. Definitions

Acceptable risk: The objective ability of the organization to continue its activities despite the occurrence of an information security risk. The threshold of risk above which information assets are at intolerable risk.

Access code: An identification and authentication mechanism that uses an individual code and password, or a substitute such as a magnetic card, smart card, or security token, to uniquely identify a user using a College information resource.

Authorization: The granting of access rights to information assets by an authority, consisting of an access privilege granted to a person, device, or entity.

Categorization: The process of determining the degree of sensitivity of information assets, taking into account the impact that a breach of the availability, integrity, or confidentiality of such College assets could have.

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

Computer equipment: Laptops, computers, minicomputers, microcomputers, computer workstations and their peripherals or accessories for reading, storing, reproducing, printing, transmitting, receiving, and processing information, and all telecommunications equipment.

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: 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.

Government information security risks: The risk of a breach in the availability, integrity, or confidentiality of government information that could affect the delivery of services to the public; the life, health, or well-being of individuals; respect for their fundamental rights to the protection of their personal information and privacy; the image of the government; or the delivery of services by other public bodies.

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: 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 lifecycle: All the stages an item of information goes through from its creation, recording, transfer, retrieval, processing, and transmission to its retention or destruction in accordance with the College's retention calendar.

Information security measures: Concrete means of partially or fully protecting the College's information assets from one or more risks (major computer network or server failure, unintentional act, malicious act such as intrusion into a computer system, etc.) and whose implementation is intended to reduce the likelihood of those risks occurring or to reduce the resulting losses.

Information security risk: The degree of exposure of information or an information system to a threat of interruption or degradation of service quality, or a threat to the availability, integrity, or confidentiality of information that could affect the delivery of services, the life, health, or welfare of individuals, the protection of their personal information, respect for their privacy, or the image of the College.

Information security standards: A series of documented processes that define how to implement, manage, and monitor various security controls. As well as providing a blueprint for mitigating risk and reducing vulnerabilities, cybersecurity standards and cybersecurity frameworks for achieving regulatory compliance. Some of these standards, without being limited to this list, includes government laws, regulations, directives frameworks as well as international well recognized standards like ISO 27000, NIST 800-60, MITRE ATT&CK and COBIT.

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.

Management framework: set of instructions in the form of policies, regulations, directives, procedures and recognized best practices and industry standards that govern the activities of an organization such as a college.

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

Members of the College community: Refers to all students, teachers, and employees of Champlain Regional College. A student who is also an employee is first, and foremost, a student. For the purposes of the Policy, the term also includes third-party contractors and service providers, guests of students and employees, union representatives, student association representatives, volunteers, sponsors, and members of the governing bodies of the College.

Software: A set of programs designed to perform a specific task on a computer. The term software is used to refer to all types of programs, including operating systems.

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

User: 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.

6. Roles and responsibilities

Information security is underpinned by an ethical approach that seeks to regulate behaviour and ensure individual accountability. Effective information security requires clear accountability at all levels of the College.

The Policy assigns the management of information security at the College to various entities, committees, and individuals based on the specific functions they perform.

6.1. Board of Governors

The Board of Governors approves and adopts the Policy and Guiding Principles and any subsequent amendments to the Policy. It also receives information security reports.

6.2. 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 Policy and associated information security management framework. The Director General is also responsible for delegating the functions of the Chief of Organizational Information Security (CSIO) and Organizational Information Security Coordinator (COMSI).

The Director General shall also:

- Support the CSIO.
- Approve official information security accountability documents.
- Authorize, on an exceptional basis, a derogation from any provision of the Policy, College's directives, or procedure that directly or indirectly affects information security and that would be inconsistent with an activity or project directly related to the mission of the College.
- Lead the Information Security Crisis Committee.

6.3. 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, they ensure compliance with and enforcement of information security laws and regulations, application of the government information security framework, and application of the Policy and associated information security management framework to their constituent college.

The Director of Constituent College shall also:

- Support the Director General in their role as the primary authority for information security.
- Support the CSIO.
- Participate in the Information Security Crisis Committee.

6.4. 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.

In this role, Corporate Affairs must work with the CSIO:

- Communicate issues and security concerns regarding the protection of personal or sensitive information to the CSIO.
- Ensure consistency and harmonization between information security, document access and privacy, including implementation of information security risk and incident management processes.
- Ensure that the standing committee on the protection of personal information is consulted to conduct a privacy impact assessment (EFVP) for any project involving the acquisition, development or redesign of an information system that involves the collection, use, disclosure, retention, or destruction of personal information.
- Work closely with managers and the CSIO to identify, manage, coordinate, and implement information security measures, regardless of medium.

6.5. Chief of Organizational Information Security (CSIO)

- The CSIO is a member of the management personnel of the College.
- The CSIO function is delegated by the Director General.
- The CSIO reports to the Director General under the Government Information Security Management Framework.

- The CSIO is responsible for the overall management of information security within their organization. They work closely with government information security stakeholders to ensure that information security requirements are met.
- The CSIO proposes to the College strategic orientations, risk assessments, action plans, security assessments, and reports on information security matters.
- The CSIO is responsible for the dissemination and implementation of the Policy.

6.6. Organizational Information Security Coordinator (COMSI)

The COMSI functions at the operational level. 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.

The COMSI represents the College on the Government Alert Network (CERT/AQ). They are responsible for applying the Threat, Vulnerability, and Incident Management (GMVI) process for the College in support of the CSIO.

The COMSI will apply appropriate response measures to any information security threat or incident, such as temporary interruption or withdrawal of access and/or services to an information system, if circumstances so require, in order to ensure the security of the information concerned.

They work with the College's CSIO to develop various strategic and tactical elements of information security:

- Maintains a registry of information security events and incidents.
- Conducts and participates in information security risk analysis.
- Manages and contributes to the implementation of the incident, reporting and, resolution management process.
- Contributes to the formal identity and access management (IAM) process.

6.7. Information Technology Services

The Information Technology Services are responsible for the application of the Policy 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 participates with the CSIO in identifying security measures to adequately protect the College's information assets in order to integrate protective measures based on the level of sensitivity of the information, taking into account regulatory, organizational process, legal, or contractual requirements.

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.

The Information Technology Services also:

- Ensure that the Policy is enforced.
- Actively participates in the risk analysis, needs assessment, and measures to be implemented in anticipation of any threat to the security of information systems.
- Collaborate with the COMSI in applying the Threat, Vulnerability, and Incident Management (GMVI) process to their college.
- Maintain a local registry of all incidents, threats, and vulnerabilities and report them immediately to COMSI.
- Participate in the implementation of all necessary information security mechanisms as determined by the College's information security strategy.
- Participate in investigations of actual or apparent violations of The Policy.
- Perform and report the results of the risk analysis required prior to all information technology projects.

6.8. Human Resources Services

In terms of information security, the Human Resources Services must:

- Conduct background checks, as appropriate, on employment candidates and information security personnel.
- Ensure that employee job descriptions include their responsibilities with regard to information security and compliance with the Policy and the information resources standards framework.
- Inform all new employees of the College and obtain their commitment to comply with the Policy and the associated management framework.
- Notify Information Technology Services of hires, position changes, and terminations to update access to College information resources in accordance with Identity and Access Management (IAM).
- Apply appropriate sanctions for violations of information security policies, regulations, directives, and codes of conduct.

6.9. 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.

In terms of security, the Material Services must:

- Control physical access to College’s premises.
- Manage physical access (keys, magnetic cards, etc.) to restricted areas (computer rooms, storage, etc.).

- Maintain, in a registry, the information necessary to track the level of access and means of access of personnel within the College (key assignment, magnetic key management system, etc.).

6.10. 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. Information asset custodians may delegate all or part of their responsibilities to another person in their department without relinquishing responsibility for the protection of those information assets.

They:

- Consult Information Technology Services for a risk analysis for all information technology projects.
- Participate in the categorization of the information under their responsibility in terms of sensitivity, availability, integrity, and confidentiality.
- Participate in all risk management activities, including assessment, determination of target level of protection, development of controls, and management of residual risk.
- 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. Examples: identity and access management, risk level management, etc.
- Participate in cybersecurity training and awareness activities and ensure that employees under their supervision actively participate in such activities.
- 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 Policy and all other elements of the information security management framework.
- Report any violations or issues related to the application of the Policy to the CSIO.

6.11. 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 Policy and all other College directives and guidelines regarding information security and use of information assets.
- Be accountable for actions resulting from the use of their identifier, access code or password, whether such actions are taken by them or by a third party, unless they can demonstrate that the actions taken by such third party were not the result of their negligence or bad faith.
- Comply with legal requirements regarding the use of products (licenses, software, packages, applications, and cloud-based services) or documents in which intellectual property rights may exist.
- Notify management of any situation that could compromise the security of information assets.
- Participate in categorizing department information as needed.
- Participate in cybersecurity training and awareness activities.
- 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.

6.12. Students

The students must:

- Comply with the Policy and all other College directives and guidelines regarding information security and use of information assets.
- Be accountable for actions resulting from the use of their identifier, access code or password, whether such actions are taken by them or by a third party, unless they can demonstrate that the actions taken by such third party were not the result of their negligence or bad faith.
- Comply with legal requirements regarding the use of products (licenses, software, packages, applications, and cloud-based services) or documents in which intellectual property rights may exist.
- 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.

7. Guiding principles

7.1. Accountability

- Everyone has a role to play in protecting information and ensuring information security.
- The effectiveness of information security measures depends in part on assigning responsibility and accountability to users.
- The College provides users with the various devices and software necessary to perform their duties as defined by the College. Users assume specific responsibility for the use of this assigned equipment and software and are therefore accountable for their actions. The College will take the necessary measures to ensure that the equipment is used properly.

7.2. Right of inspection

Since information assets belong to the College, it is within the College's discretion to determine how they are used by a user. In accordance with applicable laws and regulations, the College has the right to inspect any use of its information assets.

7.3. Information security[1]

The College adheres to the principles of best practices in information security, relies on relevant international standards to promote the use of best practices, and uses benchmarking with similar organizations or institutions.

The College also adheres to an acceptable risk-based approach by establishing an information security management framework as a means of adjusting risk through a combination of reasonable measures taken to ensure the security of information.

[1] NIST Publication SP800-53

Information security is based on the following three principles:

7.3.1. Availability

Availability ensures that authorized users of a system have timely and uninterrupted access to the information contained in that system and to the network. Information must be accessible in a timely manner and in the form required by an authorized user. Control measures must be in place to ensure this availability.

7.3.2. Integrity

Data integrity means ensuring that data has not been altered in any way during communication, whether at rest, in transit, or in memory. Physical and logical access security measures must be in place to ensure data integrity.

7.3.3. Confidentiality

Confidentiality is intended to prevent unauthorized access to sensitive information. Its goal is to ensure that information or data is accessible only to authorized individuals. The confidentiality of information must also be maintained throughout its lifecycle. Control measures must be in place to ensure confidentiality.

7.4. Categorization of information

Information is a crucial resource that must be protected throughout its lifecycle. For this reason, it is essential to maintain an up-to-date inventory of all College information assets. One of the first inputs to information security is knowledge of the sensitivity of the College's information assets. Information security categorization of information assets is a process that allows the degree of sensitivity of assets to be assessed in order to determine their level of protection.

It is important to periodically reassess the categorization of information assets to ensure that the assigned categorization is still appropriate in light of changes in legal and contractual obligations, as well as changes in the use of the data or its value to the College. This assessment should be performed by the asset custodian.

8. Management framework

The implementation of the Policy is based on the implementation of a College’s information security management framework that defines the scope of action of the various stakeholders. The management framework specifies the functional aspects of information security and enables clear objectives to be defined and appropriate accountability to be ensured.

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 Policy is based on five core management principles:

8.1. 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.

Confidential information, within the meaning of the Act respecting access to documents held by public bodies and the protection of personal information, includes personal data and any information the disclosure of which would adversely affect, in particular, intergovernmental relations, negotiations between organizations, the economy, third parties with respect to their industrial, financial, commercial, scientific, or technical information, the administration of justice and public security, administrative or political decisions and audits.

8.2. 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. A system must be in place to manage vulnerability reports from vendors or service providers so that they can be assessed and, if necessary, remediated.

8.3. 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.

8.4. 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)

8.5. 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.

9. Training, awareness and information

In particular, information security relies on the adoption of responsible behaviours and individual accountability.

Members of the College community must be made aware of:

- The College's expectations for information security and information systems.
- The consequences of a security breach.
- Their roles and responsibilities for information security.

The College is committed to educating and training users on the security of information assets on a regular basis. It is the user's responsibility to participate in these awareness and training activities.

10. Policy review

The policy will be reviewed as necessary, but at least every 5 years from the date of adoption.

11. Effective date

This policy is effective on the date of its adoption by the Board of Governors.

12. Sanctions

Any user who violates or coerces another to violate the Policy is personally liable, as is any person who, through negligence or omission, causes information to be inadequately protected.

Any College employee or student who violates the legal framework, the Policy and the resulting information security measures may be subject to sanctions in accordance with applicable laws or internal administrative or disciplinary rules (including those contained in collective agreements and College regulations) depending on the nature, severity, and consequences of the violation.

Similarly, any violation of the Policy, whether committed by a supplier, partner, guest, consultant, or third-party organization, will be subject to the sanctions provided in the contract binding them to the College or under the provisions of applicable laws and regulations.