CHAMPLAIN
REGIONAL COLLEGE

Information Security Policy

Champlain COLLEGE LENNOXVILLE

CEGEP CHAMPLAIN ST. LAWRENCE CHAMPLAIN REGIONAL COLLEGE

Champlain COLLEGE SAINT-LAMBERT

Adoption and Revision History

Board of Governors Meeting	Resolution Number	Notes
June 14, 2019	**3200**	

Table of contents

1. Preamble

The application of the Act respecting the governance and management of the information resources of public bodies and government enterprises (LGGRI) (LRQ, G-1.03) and the "*Directive sur la sécurité de l'information gouvernementale (DSI)*" requires colleges to adopt and implement an information security policy, keep it up to date, and ensure its application - the main terms of which are defined in the government directive – mainly by using information security processes to manage risks, accesses to information and incidents.

2. Purpose

The purpose of this policy is to set out how the College will meet its information security obligations.

Specifically, the College must ensure that:

- the information is available in a way that it is always accessible in a timely manner and by authorized persons only;
- information integrity is ensured so that it is neither destroyed nor altered in any way without proper authorization, and that this information medium provides the necessary stability and reliability;
- information remains confidential by restricting its disclosure and use to authorized persons, especially if it constitutes personal information.

The implementation of this policy will be guided by the institution's information security management framework.

The information security management framework will strengthen internal control processes in order to comply with government legislation and directives, as well as other risk reduction requirements associated with the protection of information.

3. Legal context

The information security policy exists in a context governed by:

- Charter of human rights and freedoms (LRQ, C-12);
- Civil code of Québec (LQ, 1991, 64);
- *"Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics"* (Decree no 261-2012);
- Act respecting the governance and management of the information resources of public bodies and government enterprises (LGGRI) (LRQ, G-1.03);

- *"Loi renforçant la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement"*;
- Act to establish a legal framework for information technology (LRQ, C-1.1);
- Act respecting access to documents held by public bodies and the protection of personal information (LRQ, A-2.1);
- Archives act (LRQ, A-21.1);
- Criminal code (LRC, 1985, C-46);
- Regulation respecting the distribution of information and the protection of personal information (A-2.1, r. 2);
- *"Directive sur la sécurité de l'information gouvernementale" (Decree 7-2014);*
- *"Cadre gouvernemental de gestion de la sécurité de l'information"*
- Copyright act (LRC, 1985, C-42);
- Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the CRTC Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23).

4. Scope

This policy refers to all information that the College holds in the course of its activities, whether it is kept by itself or by a third party. It applies to all types of support, including paper.

This policy is intended for users of information, that is, natural or legal persons who, as employees, consultants, partners, suppliers, students or public use the College information assets.

5. Definitions

Categorization

The process of assigning a value to certain characteristics of an information, qualifying the degree of sensitivity of this information and, consequently, the protection to be given to it in terms of availability, integrity and confidentiality.

CERT/AQ

Computer Emergency Response Team/Area Quebec (*Équipe de réponse aux incidents de sécurité de l'information de l'Administration Québécoise*)

College

Refers to Champlain Regional College.

Confidential information

Information whose access is subject to one or more restrictions, including those provided for in the Act respecting access to documents held by public bodies and the protection of personal information, which are the implications on intergovernmental relations, negotiations between public bodies, the economy, the administration of justice and public safety, administrative or political decisions and auditing.

Confidentiality

The characteristic of an information to be accessible only to designated and authorized persons or entities.

Continuity plan

The set of planning measures established and implemented to maintain (and restore when required) the availability of information essential to the realization of critical College activities.

Custodian of Information

The custodian of information is the individual with managerial authority within a department, or a service, whether pedagogical or administrative, whose role is to ensure the accessibility, use and the security of information assets under the responsibility of that department, or service.

Incident

An event that affects or is likely to impair the availability, integrity or confidentiality of information, or more generally to the security of information systems, including interruption of services or a reduction in their quality.

Information or information asset

It consists of personal information of students and employees; professional information subject to intellectual property rights (teachers and researchers); and, finally, strategic or operational information for the administration or governance of the College.

Information lifecycle

All the steps that information goes through, from its conception to its recording, its transfer, consultation, processing and transmission, until its permanent preservation or destruction, in accordance with the College conservation calendar.

Information security management framework

The information security management framework strengthens internal control processes by providing reasonable assurance of compliance with government legislations and directives, as well as other risk reduction requirements associated with the protection of information.

International standards

Standards of best practice in particular domain, established by international organizations such as the International Organization for Standards (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27002:2013 (Information technology – Security techniques – Code of practice for information security controls) is of particular relevance for this policy.

Personal information

Information concerning a natural person, which makes it possible to identify him/her. A personal information, which is considered public under a law, is not considered as personal information for the purposes of this policy.

User

Refers to any natural or legal person who uses the information assets.

6. Guiding principles

The College's actions in the area of information security are guided by the following principles:

a) ensuring that an inventory of information assets is maintained that includes the information to be protected, those responsible for that information, and the security measures in place to protect it;

b) using relevant international standards to implement best practices and establishing benchmarks using similar organizations and institutions;

c) adhering to an acceptable risk-based approach by establishing an information security management framework as a means of adjusting the risk, through a combination of reasonable measures put in place to ensure the security of information;

d) strictly protecting personal information and other confidential information throughout its lifecycle;

e) adhering to an ethical approach aimed at regulating conduct and individual accountability where those with access to information are responsible for its confidentiality, availability and integrity;

f) ensuring that each employee has access to the minimum information required to perform their normal duties;

g) communication with information users about threats to information assets and the importance of applying security measures, as well as recognizing security incidents, and taking appropriate actions;

h) ensuring that business continuity plans are in place to restore essential services on a timely basis.

7. Management framework

The effectiveness of information security measures requires the clear attribution of roles and responsibilities to the various College stakeholders through the implementation of a security management framework that includes adequate accountability.

Information security practices and solutions must be periodically reviewed to consider not only legal, organizational, technological, physical and environmental changes, but also evolving threats and risks.

This information security policy is structured around three fundamental management orientations. These areas are:

- access management;
- risk management;
- incident management.

7.1. Access management

Access management must be supervised, monitored and recorded to ensure that access, disclosure and use of information is strictly reserved to authorized persons. These measures are taken to protect the integrity and confidentiality of data and personal information.

The effectiveness of information security measures relies on individual accountability and the distribution of responsibilities to employees at all levels of the College.

7.2. Risk management

A categorization of “up-to-date information assets” supports risk analysis by identifying the value of the information to be protected.

Risk analysis also guides the acquisition, development and operation of information systems, specifying the security measures to be implemented for their deployment in the College environment. Information security risks management is part of the overall College risk management process. Government-wide risks are reported in accordance with the *Directive sur la sécurité de l’information gouvernementale (DSI)*.

The level of protection of the information is established according to:

a) the nature of the information and its importance;

b) probability of accidents, errors or malice to which it is exposed;

c) possible resulting consequences of a risk;

d) the level of risk acceptable to the College.

7.3. Incident management

Information security measures are implemented to ensure the continuity of College services. In this regard, the necessary measures are implemented to achieve the following goals:

- limit the occurrence of information security incidents;
- adequately manage these incidents to minimize their impact and restore activities or operations in a timely matter.

Government-wide information security incidents are reported in accordance with the *Directive sur la sécurité de l'information gouvernementale (DSI)*. (to the CERT/AQ)

The College may exercise its powers and prerogatives with respect to any improper use of the information it holds or of its information systems.

7.4. Roles and responsibilities

This policy assigns the College information security management to bodies, individuals and committees based on the particular duties they perform.

7.5. Board of Governors and Executive Committee

The Board of Governors adopts the Information Security Policy and its amendments. It is regularly informed of the College's information security initiatives. The Board is responsible for the application of this policy.

The Executive Committee may make decisions as determined by the Board.

7.6. Director General's Advisory Committee (DGAC)

The Director General's Advisory Committee (DGAC) determines measures to promote the implementation of this policy. Thus, it determines the strategic orientations, the action plans and the risks assessments of College information. It may also determine guidelines and procedures that clarify or support the application of this policy.

7.7. Information Resources Governance Committee

The purpose of the Information Resources Governance Committee is to assist the Information Security Officer (RSI) with the implementation of the information security management framework and other items that may be required to protect the College and to comply with the regulations. It is a tactical and operational committee.

This committee is responsible for developing, implementing and maintaining the information security management framework, the action plans and the information security risks assessments, the awareness-raising or training activities as well as any proposals for action on information security. It is also a forum for exchanges between committee member and/or observation of the evolution of information security.

The committee consists of the College employees who will be directly involved in the security of information from each of the campuses, duly named by the Campus Directors.

7.8. Director General

The Director General oversees the application of this policy and is responsible for:

a) overseeing the Information Security Officer (RSI) in carrying out this individual's mandate;

b) delegating certain responsibilities to the Secretary General for the management of information;

c) makes recommendations to the Board of Governors regarding the adoption of strategic directions, risk assessments, action plans, information security health assessments, accountability on information security;

d) exceptionally authorize a derogation from any of the provisions of this policy, a directive or an institutional procedure having a direct or indirect impact on the security of information and which would be incompatible with an activity or project directly related to the mission of the College;

e) authorizing an investigation where there is, or could be, an actual or apparent violation of this policy;

f) ensuring the maintenance of the register of exemptions and the register of cases of contraventions to this policy.

7.9. Information Security Officer (RSI)

The responsibilities of the RSI are delegated to a manager named by the Board of Governors upon the recommendation of the Director General. The RSI reports to the Director General as defined in the *Cadre gouvernemental de gestion de la sécurité de l'information*. This person implements the information security management framework and ensures that the level of maturity in information security management practices meets the College's needs.

The RSI:

- develops and proposes the College's information security program and reports its implementation to the Board of Governors;
- makes recommendations with respect to the needs, priorities, directions, action plans, guidelines, directives, procedures, initiatives and good practices in information security and on updates to this policy accordingly;
- ensures the coordination and consistency of the College's actions in the area of information security, by advising the custodians of information in the organization;
- produces the College action plans, health assessment and accountability reports on

information security;
- proposes provisions for compliance with information security requirements to be incorporated into service agreements and contracts;
- ensures that the College reports any government-related information security risks and incidents (CERT/AQ);
- collaborates in the development of the content of the communication plan, the information security awareness and training program, and ensures their implementation;
- conducts investigations into serious transgressions pertaining specifically to this policy upon authorization of the Director General;
- ensures monitoring of ongoing changes in standards, laws and regulations, government practises and technological advances related to information security.

7.10. Information technology services

In the area of information security, the information technology services ensure that information security requirements are met throughout the information systems as well as in the execution of development projects or acquisition of information systems. The information technology services:

- actively participates in risk analysis, needs assessments and measures to be implemented, and anticipates any security threats to information systems that use information technology;
- applies appropriate response measures to any information security threat or incident, such as, interruption or temporary revocation of information system services to ensure the security of the stored information;
- participates in investigations relating to actual or apparent violations of this policy upon authorization of the Director General.

7.11. Material services

Material Services, along with the RSI, participates in the identification of physical security measures that adequately protect the information assets of the College.

7.12. Human Resources

The Human Resources communicates this policy to every employee of the College and obtain a signed commitment to comply with it.

7.13. Custodian of Information

The custodian of information may delegate all or part of their responsibility to another member of their department, or service.

The custodian of information is responsible for:

- informing the employees under their authority as well as the third parties with whom the service interacts, of the information security policy and management framework, in order to raise awareness and the need to comply with this policy;
- actively collaborating in the categorization of information and in the risk analysis;
- seeing to the protection of the information and information systems under their responsibility and ensuring that these are used by employees under their authority in accordance with this policy and any other element of the management framework;
- ensuring that information security requirements are taken into account in any acquisition process and any service contract under their responsibility and ensuring that any consultant, supplier, partner, guest, organization or external firm respect this policy and any other element of the management framework;
- reporting any information security threats or incidents to the Information Technology Services;
- collaborating in the implementation of any measure to improve the security of information or to remedy an information security incident as well as any information security audit operation;
- reporting to the Director General any problem associated with the application of this policy, including any actual or apparent violation by an employee in the application of this policy.

7.14. Users

The responsibility for the security of information rests with all users of the College.

Any user who accesses, consults or deals with or manages information is responsible for its use and must proceed in such a way as to protect it.

To this end, the user must:

- comply with this policy and any other directive of the College on information security and its use;
- use the access rights granted and authorized, the information and the information systems that are made available solely in the course of their duties and for the purposes for which they are intended;
- participate in the categorization of information within their department, or service;
- respect the security measures in place, such as but not limited to, not circumventing them, nor changing their configuration or disabling them;
- inform the information asset custodian of any incident likely to constitute a violation of this policy or to constitute a threat to the security of the College;

- collaborate in any intervention to identify or mitigate a threat to information security or an information security incident.

As a result, all College users must comply with the policies and directives in force in the course of their professional or academic activities when sharing information assets, information technology or information systems.

8. Awareness and information

Information security relies on the regulation of conduct and individual accountability. In this regard, College employees and students must be aware of:

- the security measures, program, policy applicable to the College information and systems;
- the consequences of a breach of security;
- their role and responsibilities in this area.

To this end, awareness and training activities are to be offered periodically. In addition, explanatory documents are to be made available and disseminated on the College website.

9. Sanctions

Any user violating this policy may be held personally responsible; the same shall apply to a person who, through negligence or omission, causes a situation that renders the information inadequately protected.

Any College employee or student who contravenes the legal framework of this policy and its related information security measures is subject to sanctions depending on the nature, severity and consequences of the violation, in accordance with applicable laws or internal disciplinary rules (including those of the collective agreements and the college regulations).

Similarly, any violation of this policy by a supplier, partner, guest, consultant, or external organization is punishable by the penalties provided for in the contract binding their relationship to the College or under provisions of the applicable laws and regulations.

10. Dissemination and updating of this policy

The RSI, assisted by the Information Resources Governance Committee, is responsible for disseminating and updating this policy. This policy will be reviewed no later than three (3) years after its initial adoption and at least every five (5) years thereafter.

Notwithstanding the review cycle, this policy may also be updated following changes to current legislations related to information security.

11. Effective date

This policy comes into force on the date of its adoption by the Board of Governors.