VANIER
CÉGEP/COLLEGE

# Information Security Policy

Approved by the Vanier College Board of Directors: February 21, 2017

# Table of Contents

## 1. Preamble

This policy was developed pursuant to section 7 a) of the Quebec Government's ***Directive sur la sécurité de l'information gouvernementale*** that requires public bodies to adopt and implement an information security policy, keep it up-to-date and ensure its application.

## 2. Definitions

**Information Assets**

All active, semi-active and inactive documents created or received by College personnel in the pursuit of their duties regardless of their nature (administrative, financial, legal or otherwise), media (hard copy, digital, audiovisual, web or otherwise) and the format in which they are produced.

**Confidentiality**

A property of data or information such that it is accessible only to designated or authorized persons or entities.

**The College**

Vanier College of General and Vocational Education.
A non-profit legal person.
(Une société, aussi appelée une personne morale, sans but lucratif).

**Information Lifecycle**

Stages through which every document or record goes through, from its creation, storage, transfer, consultation, processing and transmission, to its retention or destruction, in accordance with the Vanier College retention schedule.

**Availability**

A property of data or information such that it is accessible in a timely manner in the format required by an authorized person.

**Integrity**

A property of data or information such that it does not undergo any alteration or destruction without authorization and is kept on a medium that provides stability and durability.

**Information security management framework**

A collection of objectives and practices based on industry I.T. governance standards.

## 3. Legal and administrative context

This Information Security Policy is implemented in conformity with the following legislation:

- Charter of Human Rights and Freedoms, CQLR c C-12
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics

- An Act Respecting the Governance and Management of The Information Resources of Public Bodies and Government Enterprises, CQLR c G-1.03
- An Act to Establish a Legal Framework for Information Technology, CQLR c C-1.1
- An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, CQLR c A-2.1
- Archives Act, CQLR c A-21.1
- Public Administration Act, SQ 2000, c 8
- Public Service Act, CQLR c F-3.1.1
- Canadian Human Rights Act, RSC 1985, c H-6
- Criminal Code, RSC 1985, c C-46
- Copyright Act, RSC 1985, c C-42
- Regulation respecting the distribution of information and the protection of personal information, CQLR c A-2.1, r 2
- Directive sur la sécurité de l'information gouvernementale
- Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire

## 4. Policy objective

The purpose of this policy is to affirm Vanier College's commitment to fully comply with its information security obligations, regardless of its medium or means of communication. More specifically, it is about ensuring the availability, integrity and confidentiality of information throughout its lifecycle.

## 5. Scope of application

This policy applies to data security, regardless of its form, digital or otherwise. It covers the areas of information technology, physical security and document management.

### 5.1 Data and information assets

This policy is applicable to the following categories of information:

1. Information owned or used by the College;
2. Information owned by the College and used or held by a partner, a supplier of goods and services or another stakeholder;
3. Information owned and used by a partner, a supplier of goods and services, or any other stakeholder on behalf of the College;
4. Information that is not owned by the College, but that is held there.

### 5.2 People

This policy is intended for all users, that is, anyone who has access to the data and/or information assets of the College regardless of employment status, including contract workers and exchange personnel as well as to any/all partners, suppliers or other stakeholders.

### 5.3 Activities

Any activity involving the use, disclosure, or preservation, in any form, of data or information assets owned by or used by the College is covered by the policy, whether on premises, off site or remotely.

This policy applies from the earliest phase of design or creation of the data or information asset and during the development, realization or modification of the asset or any associated business processes.

#### 5.3.1 Operation and administration of the information technology infrastructure

The security of information technology infrastructure must be supported by tools, practices and measures to monitor and regularly update the College's operating systems, application software and equipment, including specifically but not limited to:

- Patches and updates provided by software and hardware suppliers;
- An annual assessment of risks related to information technology.

#### 5.3.2 Disposal of old computer systems and equipment

The rules for the safe destruction of any microcomputer equipment declared as "surplus movable property" and any removable computer media intended for disposal or entrusted to a supplier must be applied in a timely manner and in accordance with the Directive concernant le traitement et la destruction de tout renseignement, registre, donnée, logiciel, système d'exploitation ou autre bien protégé par un droit d'auteur, emmagasiné sur un équipement micro-informatique ou sur un support informatique amovible of the Secrétariat du Conseil du trésor.

The same applies to any microcomputer or removable media equipment entrusted to a supplier for repair, maintenance, destruction or retrieval of the information stored therein.

#### 5.3.3 Document management and destruction

The College is subject to the Archives Act, CQLR c A-21.1 and the records management policies established by the Bibliothèque et Archives nationales du Québec (BAnQ).

The College is obliged to apply the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, CQLR c A-2.1, in particular, section 63.1, which states that "*A public body must take the security measures necessary to ensure the protection of the personal information collected, used, released, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.*"

Therefore, appropriate action will be taken to ensure that College document availability and retention is in accordance with the College's BAnQ approved document classification and retention plan.

### 5.3.4 Physical security of buildings and premises

The College will ensure the physical security of College premises where data and information assets are stored. The College will establish and update an access list of authorized personnel that it is verified and updated periodically or during a significant organizational change.

## 6. Guiding principles

### 6.1 Rationale for information security

The objective of information security is to promote confidence in the College and the services it renders and to contribute to the achievement of the College's mission. It also aims to ensure the integrity, durability, reliable accessibility and confidentiality of information.

### 6.2 Protection of information

Information security must be ensured throughout its life cycle and the means used to ensure it must be proportional to its value and the risks to which it is exposed. Thus, any information that the College holds, processes or transmits must be subject to security measures designed to:

- Ensure that information is accessible at all times in the format required by an authorized person;
- Ensure the integrity of the information so that it does not undergo any alteration or destruction without authorization and is kept on a medium that provides stability and durability;
- Restrict access or disclosure to only those authorized to access it, thus ensuring strict, controlled and confidential use;
- Confirm the identity of a person or the identification of a document or device (authentication) in order to ensure appropriate access;
- Ensure that any confidential information is protected from unauthorized disclosure, access or use. For the purposes of the Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, CQLR c A-2.1 , confidential information is considered to be personal information and any information the disclosure of which would have harmful implications for any of the following: intergovernmental relations, negotiations between public bodies, the economy, third parties with respect to their industrial, financial, commercial, scientific or technical information, the administration of justice and public safety, administrative or political decisions and verification.

### 6.3 Information security awareness and training

The College undertakes, on a regular basis, to raise awareness and train users on the security of information assets, the consequences of a security breach and their role and responsibilities in this regard.

### 6.4 Right of inspection

The College shall exercise, in conformity with the legislation and the regulations in force, the right of inspection on any use of its informational assets.

### 6.5 Responsibility and accountability

The security of informational assets is supported by an ethical approach aimed at ensuring the regulation of conduct and individual accountability.

The effectiveness of information security requires clear accountability at all levels of the organization, including partners and suppliers within the College. This will entail the implementation of internal information security management framework and defined processes that ensures adequate accountability.

### 6.6 Compliance with applicable laws, regulations and standards

In addition to the College's information security management framework and its related documents, the College must comply with applicable laws, regulations and standards.

All users must comply with the requirements for the use of products, documents and information, in respect of which there may be an intellectual property right. Thus, the use of proprietary software and free software must comply with the Copyright Act, RSC 1985, c C-42.

I.T. Services will ensure that its software licenses are properly managed. Only software provided by the College must be used.

The use of any other software must be subject to a specific authorization from the College's *information security officer (Responsable de la sécurité de l'information - RSI)*.

## 7. Obligations of key stakeholders in information security

This policy sets out information security obligations, including, but not limited to the College, the College information security officer (RSI), information owners, administrators and users.

**The College**

Primarily responsible for the security of the information under its authority.

**The Information Security Officer (RSI)**

Assists the College in identifying strategic directions and priorities for action.

**The custodian of the information**

An employee designated by the College and reporting to the administrative unit of which they are a part, whose role is, among other things, to ensure the security of the information and its related resources.

**Managers**

Responsible for the implementation of the provisions of this policy with the personnel under their authority.

**Users**

Responsible for complying with government directives, this policy and the rules applicable to them, by signing the attached statement of commitment.

The roles and responsibilities assigned to other stakeholders as well as the internal structures for coordination and consultation on information security shall be defined in the information security management framework, which complements this policy.

## 8. Obligation of users

The College shall have an incident reporting and management process.

### 8.1 Reporting

Every user has an obligation to protect the information assets made available to him by the College. To this end, the user shall report, without delay, to his manager or to I.T. Support Services any act likely to represent a real or presumed infringement of the security of the information. The *coordinator of security incident management (Coordonnateur sectoriel de gestion des incidents - CSGI)* must also be notified when a security incident occurs, in order to determine the measures to be taken to resolve the problem, as may be required. Information security incidents must be recorded in an incident log, analyzed and classified according to severity.

## 9. Sanctions

When a user contravenes this policy or its attendant directives, they may incur disciplinary, administrative or legal action, depending on the severity of their action. Such measures may include suspension of privileges, reprimand, suspension, dismissal or otherwise, in accordance with the provisions of collective agreements, other agreements or contracts.

The College may transmit to any judicial authority the information gathered and which leads it to believe that an infringement of any law or regulation in force has been committed.