No. BOG-DG-01

Title:	**FRAMEWORK POLICY ON INFORMATION SECURITY**
CLASSIFICATION:	Director General
FIRST ADOPTED:	April 13, 2018

Objectives

The Act Respecting the Governance and Management of Information Resources and the Directive on the security of governmental information requires the adoption of a framework policy for information security.

This framework policy ensures that adequate measures are in place to guarantee:

- *Confidentiality*, by limiting disclosure and use of information by authorized persons only;
- *Integrity*, by ensuring durability of information and preventing its unwarranted destruction or alteration;
- *Availability,* by securing access to information in a timely manner and to authorized individuals only.

Article 1 Legal context

This framework policy is applied in accordance to applicable laws, bylaws, regulations and policies, including without limitation:

- *Act Respecting the Governance and Management of Information Resources* (CQLR, G-1.03) and *Directive on the security of governmental information*
- The *Government security management framework* (*Cadre gouvernemental de gestion de la sécurité de l'information*)
- *Act to establish a legal framework for information technology* (CQLR, C-1.1);
- *Act respecting Access to documents held by public bodies and the Protection of personal information* (CQLR, A-2.1)
- *Archives Act* (CQLR, A-21.1)
- *Charter of human rights and freedoms* (CQLR, C-12)
- *Civil Code of Quebec* (CQLR CCQ-1991)
- *Criminal code* (RSC, C-46)
- The College *IT Security Policy* (IST-01) and *IT Incident Management Policy* (IST-05)

Article 2 Scope of application

Any information that the College collects, produces or retains in the course of its activities is subject to this framework policy. The information may be stored electronically or on paper, and be physically located inside or outside the premises.

The policy is applicable to employees, students, third parties who use this information.

Article 3 Security management framework

The management of information security is based on three components: access management, risk management and incident management.

3.1. Access management

Measures are in place to ensure that access to, disclosure of and use of information is strictly reserved to authorized persons. These measures protect the integrity and confidentiality of information, with particular attention to personal information.

The effectiveness of access management relies on the assignment of responsibilities and accountability to all levels within the College.

3.2. Risk management

The management of information security risks is part of the College's overall risk management process.

Risk analysis guides the acquisition, development and operation of information systems, specifying the security measures to be implemented for their deployment in the College environment..

3.3. Incident management

The College deploys measures to ensure the continuity of its services. In this regard, it shall put in place the measures necessary to achieve the following objectives:

- limit the occurrence of information security incidents;
- adequately manage these incidents to minimize the consequences and restore operations.

Incidents of government-wide proportion are defined in the *Directive on the security of governmental information as events that compromise the availability, integrity or confidentiality of governmental information, and which require a concerted intervention*. They are reported as prescribed in the Directive.

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

Article 4 Roles and responsibilities

4.1. Board of Governors

The Board of Governors adopts this framework policy and its amendments, and delegates its application to the Director General. It also appoints the Information Security Officer, as prescribed in the *Government security management framework*.

4.2. Director General

The Director General is responsible for the application of this policy. In particular, the Director General:

- Recommends this policy and its amendments to the Board;
- Oversees the Information Security Officer in carrying out the mandate;
- Informs the Board of actions related to information security, such as risk assessments, action plans, etc.;
- Exceptionally authorizes a derogation from this policy;
- Applies sanctions related to breaches of this policy.

4.3. Information Security Officer

In addition to the mandate defined in the *Government security management framework*, the Information Security Officer acts as a liaison with the Ministry, and assists the Director General in the implementation of this policy. In particular, the Information Security Officer:

- Recommends this policy and its amendments to the Director General, as well as other directives, action plans, etc. where appropriate;
- Conducts investigations into possible cases of breach of the policy
- Reports breaches of the policy to the Director General
- Coordinates and ensures consistency of actions between information owners, also considering aspects of contract management, access and protection of personal information, and document management;
- Ensures that the College participates in the governmental process for risk management and incident reporting;
- Establishes the security management framework;
- Establishes a training and awareness program for information security.

4.4. Academic Dean and Directors

The Academic Dean and the Directors are responsible to ensure that the operations of their units comply with the policy, and that an effort proportionate to the risk be deployed to protect the information. They actively collaborate with the Information Security Officer to assess risk, to implement new measures and to report any potential threat that comes to their attention.

The following Directors have additional responsibilities:

- The Director of Information Systems and Technology ensures that security requirements are met throughout existing information systems as well as in the acquisition or development of new systems;
- The Director of Information Systems and Technology applies appropriate response measures to an information security threat or incident, such as interruption or temporary revocation, where circumstances require;
- The Director of Plant and Facilities is involved in the identification of physical security measures to adequately protect the information assets of the College;
- The Director of Human Resources obtains a commitment from all new College employees to comply with this policy.

4.5. Users

When accessing or processing information, users must proceed in such a way to protect it. They must use their access solely for the purposes for which it is intended. They must report incidents which could constitute a threat to information security and collaborate in investigations.

4.6. Information Security Committee

The goal of this working committee is to assist the Information Security Officer to implement the policy, the security management framework, the action plans, as well as training and awareness programs.

Article 5 Sanctions

Any employee or student who contravenes this policy or its related information security measures, is subject to sanctions depending on the nature, severity and consequences of the violation under bylaw or applicable disciplinary rules (including those of the collective agreements and the rules of the college). The employee or student may be held personally responsible, even in case of negligence or omission, if the violation causes the information to be inadequately protected.

Similarly, any violation of this policy perpetrated by a third-party organization or an individual who is not an employee or student, is punishable by the penalties provided for in the contract binding it to the College or under the provisions of the applicable legislation.

Article 6 Final provisions

This policy is effective on the date of adoption.