commission scolaire
DU LITTORAL

IDENTIFICATION CODE
POL19-081

TITLE: INFORMATION SECURITY POLICY

EFFECTIVE DATE	REQUIRED AUTHORIZATION	RESPONSIBLE FOR MONITORING
May 22, 2019	**Administrator**	**Secretary General**

ROADMAP

	DATE	AUTHORIZATION
ADOPTION	May 22, 2019	Administrator

commission scolaire
DU LITTORAL

Table of Contents

1. BACKGROUND

The Act respecting the governance and management of information resources of public bodies and government enterprises (ARMIR) (RLRQ, chapter G-1.03) and the Directive on the security of government information (DSGI), a directive of the Secrétariat du Conseil du trésor, applicable to the Commission scolaire du Littoral, creates obligations for educational institutions in their capacity as public bodies.

Thus, the GISD requires the School Board to adopt, implement, maintain and ensure the application of an information security policy - the main terms and conditions of which are defined in the directive - using, in particular, formal information security processes that ensure risk management, access to information management and incident management. As stipulated in the Appointment Guide, an Information Security Officer (ISO) and a Sector Incident Management Coordinator (SIMC) must be designated.

This policy allows the School Board to respect its obligations, preserve its reputation, respect the laws and reduce risks by protecting the information it has created or received (of which it is the custodian). This information related to human, material and financial resources is accessible in digital and paper formats, the risks of which may affect its availability, integrity or confidentiality may have consequences related to:

- The life, health or well-being of people;
- The breach of personal information and privacy;
- The provision of services to the population;
- The image of the School Board and the government.

2. OBJECTIVE

The purpose of this policy is to assert the School Board's commitment to fully meet its obligations with respect to information security, regardless of its support or means of communication.

More specifically, the School Board must ensure that:

- The availability of information so that it is accessible in a timely manner and in the manner required by authorized persons;
- The integrity of the information so that it is not destroyed or altered in any way without authorization, and that the support of this information provides it with the desired stability and durability;
- Confidentiality of information, by limiting its disclosure and utilization to authorized persons only, especially if it is personal information.

Consequently, the School Board is implementing this policy in order to guide and determine its vision, which will be detailed in the Information Security Management Framework.

3. LEGAL AND ADMINISTRATIVE FRAMEWORK

The Information Security Policy is mainly set in a context governed by:

- The Charter of Human Rights and Freedoms (RLRQ, chapter C-12);
- The Education Act (RLRQ, c. l-13.3);
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (RLRQ, c. A-21.1, r.2);

- The Civil Code of Quebec (RLRQ, chapter CCQ-1991);
- The Policy Framework on the Governance and Management of Information Resources of Public Bodies;
- The Act respecting the governance and management of information resources of public bodies and government enterprises (RLRQ, c. G-1.03);
- The Act respecting the legal framework for information technology (RLRQ, chapter C-1.1);
- The Act respecting access to documents held by public bodies and the protection of personal information (RLRQ, chapter A-2.1);
- The Criminal Code (RTA, 1985, chapter C-46);
- The Regulation respecting the dissemination of information and the protection of personal information (RLRQ, chapter A-2.1, r. 2);
- The Directive on the Security of Government Information;
- The Copyright Act (R.S.C., 1985, chapter C-42);
- Computer and Network Usage Policy
- Guidelines for Using Social Media;
- Policy Regarding on the Use of Social Media.

4. FIELDS OF APPLICATION

This policy is intended for information users, that is, all employees, any physical or legal person who, as an employee, consultant, partner, supplier, student or public, use the School Board's information assets..

The information in question is that which the School Board holds in the course of its activities, whether it is stored by itself or by a third party. The format of the information concerned is electronic and paper.

5. GUIDING PRINCIPLES

The guiding principles that guide the School Board's actions in information security are as follows:

- Ensure that they are familiar with the information to be protected, identify who is responsible for it and its security features;
- Recognize the importance of the Information Security Policy;
- Recognize that the technological environment is constantly changing and interconnected with the world;
- Protect information throughout its life cycle (creation, processing, destruction);
- Ensure that each employee has access to the minimum information required to perform their normal duties;
- The use of IT resources by users must be limited to the professional functions assigned to them. A personal activity is tolerated as long as it is of short duration. Personal information must not be uploaded to the computer by the user, as it could introduce a virus and, as a result, the School Board could destroy this information without the user's consent.

6. RISK MANAGEMENT

An up-to-date categorization of 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, by specifying the security measures to be implemented for their deployment in the School Board environment. Information security risk management is part of the School Board's overall risk management process. Government-wide risks are reported in accordance with the GISD.

The level of information protection is established according to:

- The nature of the information and its importance;
- The probability of accidents, errors or malicious acts to which it is exposed;
- The consequences of the materialization of these risks;
- The level of risk acceptable to the School Board.

7. INCIDENT MANAGEMENT

The School Board deploys information security measures to ensure the continuity of its services. In this regard, it puts in place the necessary measures to achieve the following goals:

- Limit the occurrence of information security incidents;
- Properly manage these incidents to minimize their consequences and restore activities or operations.

Government-wide information security incidents are reported to DSSE in accordance with the GISD.

In managing incidents, the School Board may exercise its powers and prerogatives with respect to any inappropriate use of the information it holds or its information systems.

8. GUIDELINES

8.0 Access management

A system of access management must be developed, monitored and controlled to ensure that the availability, integrity and confidentiality of information are protected. This management should include the approval, revalidation and destruction of these accesses and keep this evidence for future audits. The IT Resources Department is responsible for the application of this measure for digital management and the General Secretary's Office is responsible for the application of this measure for paper based management.

8.1 Vulnerability management

The School Board is deploying measures to keep the software in its computer equipment up to date in order to keep vulnerabilities as low as possible and reduce the chances of a cyber-attack. A measure to notify vulnerabilities from suppliers must be put in place to correct them. The IHR is responsible for the application of this measure.

8.2 Backup copy management

The School Board must develop a backup strategy to protect against data loss. This strategy should include retention of copies, error alerts when copies are taken and tests to restore these copies at an appropriate frequency. The IHR is responsible for the application of this measure.

commission scolaire
DU LITTORAL

8.3 Business continuity

The School Board must develop a business continuity strategy in the event that an incident causes the Board to stop providing services. This strategy should be tested at an appropriate frequency and deviations corrected. The Computer Resources Department is responsible for the application of this measure.

8.4 Protection of the network perimeter

The School Board must implement intrusion testing and vulnerability scanning exercises to identify entry points that may give inappropriate access to individuals or malicious programs. In addition, an intrusion prevention and detection system should be put in place to increase the level of protection. Also, by segmenting its network, the School Board limits the chances of spreading a virus or attack. The Computer Resources Department is responsible for the application of this measure.

8.5 Use of a personal device (b.y.o.d.)

A directive on the use of a personal device (iPad, smartphone, laptop, etc.) in the performance of professional duties will be developed to effectively manage this practice. School Board data must be protected.

An agreement must be signed between the School Board and the users listing their respective responsibilities and the procedures to be put in place in the event of the theft or loss of the device. The Computer Resources Department is responsible for the application of this measure.

8.6 Protection of paper-based information assets

The School Board must have processes in place to protect the assets of paper information. A notion of own office must also be introduced. These paper assets can be transported and produced in several copies. The concepts of creation, organization, protection, dissemination and disposition must be considered in the development of these processes. Each department of the School Board is responsible for this application.

8.7 Protection of digital information assets

The School Board must have processes in place to protect digital information assets. The notion of classification, archiving, preservation and destruction must be considered in the development of these processes. Each department of the School Board is responsible for this application.

8.8 Supplier management

The School Board must put in place a process to manage its suppliers to ensure that they will not cause incidents, disclosures or data loss or introduce viruses on its network. To do so, an agreement must be signed with the supplier stipulating that it undertakes to meet the School Board's cybersecurity requirements. This agreement must also include the objectives regarding these requirements and the levels of service expected by this supplier. The managers of administrative services, schools and centers are responsible for the application of this measure.

9. AWARENESS AND TRAINING

Information security is based in particular on the regulation of conduct and individual responsibility. In this regard, the School Board's employees must be trained and made aware of this:

- The security of the School Board's information and information systems;
- To the security guidelines;
- To risk management;
- Incident management;
- To existing threats;
- The consequences of a security breach;
- Their role and responsibilities in this regard.

To this end, awareness and training activities will be offered. In addition, explanatory documents will be made available to those affected by this policy.

10. PENALTY

Any School Board employee who contravenes the Information Security Management Framework or this policy and the information security measures resulting from it, is subject to sanctions depending on the nature, gravity and consequences of the contravention, pursuant to the law or the collective labour agreements and regulations of the School Board.

Suppliers, partners, guests, consultants or external organizations are also subject to sanctions.

11. DISSEMINATION AND UPDATING OF THE POLICY

The IT Services, assisted by the Information Security Working Committee, ensures that the policy is disseminated and updated.

The Information Security Policy will be reviewed periodically as updates are made.

12. EFFECTIVE DATE

This policy is effective the day following its adoption.