COMMISSION SCOLAIRE EASTERN SHORES
EASTERN SHORES SCHOOL BOARD

INFORMATION SECURITY POLICY

ES-246

Adopted on: February, 18, 2020 Resolution C20-02-528

1. PREAMBLE

The coming into force of the *Act, the governance and management of information resources of public bodies and government enterprises (LGGRI)* (L. R. Q. , C. G-1.03) and the *Directive on the security of government information (DSIG)* (C . T. - Decree 7-2014) creates new obligations for school boards in their capacity as public bodies.

While the LGGRI is subjecting school boards to a new approach to governance of information resources, the DSIG sets the expectations and milestones. They are supported by various management frameworks that were issued by the *Conseil du trésor* and by a strategic approach. These frameworks oblige school boards to adopt, implement, maintain and ensure the application of an information security policy, the main terms of which are defined in the directive, using, among other things, formal information security processes that ensure risk, access, and incident management. This requires that two roles are minimally filled within each school board:

1. One (1) Information Security Officer (ISO), and
2. Two (2) Incident Management Sector Coordinators (IMSC).

This policy enables Eastern Shores School Board (ESSB) to fulfill its mission, preserve its reputation, respect the laws and reduce risks by protecting the information it creates or collects in the context of its activities and of which it is guardian. This information related to human, material, educational, technological and financial resources, is accessible in both digital and non-digital formats. Risks threatening the accessibility, integrity and confidentiality of information can have various consequences that compromise:

- The life, health or well-being of people,
- The protection of personal information and privacy;
- The delivery of services to the population;
- The image of the school board and the government.

The LGGRI and DSIG put in place a framework that allows for the management of information throughout its life cycle, including its permanent preservation or its destruction.

2. GENERAL OBJECTIVES

The purpose of this policy is to affirm ESSB's commitment to fully meet its obligations with respect to the security of the information it holds in the course of its activities, whatever its' medium or where it is stored. More specifically, the school board must ensure:

- <u>The availability</u> of information so that it is available in a timely manner and in the manner required by the authorized individual,
- <u>The integrity</u> of the information, so that it is neither destroyed nor tampered with in any way without authorization and that the medium used to store it provides the desired stability and sustainability,
- <u>The confidentiality</u> of information to limit disclosure and use to authorized individuals, especially when it constitutes personal information.

Therefore, ESSB adopts this policy in order to guide and define its vision, which will be detailed in a management framework of information security.

3. LEGAL AND ADMINISTRATIVE FRAMEWORK

This policy is governed primarily by the following:

- The *Education Act* (RSQ, chapter I-13.3);
- The *Charter of Human Rights and Freedoms* (L. R. Q . , C. C-12) ;
- The *Civil Code of Quebec* (LQ, 1991, chapter 64);
- The *Archives Act* (RSQ, chapter A-21.1), including the *Regulation respecting the retention schedule, the transfer, deposit and disposal of public records* (r.1) ;
- The *Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (RSQ, chapter A-2.1);
- The *Act respecting the governance and management of information resources of public bodies and government enterprises* (RSQ, chapter G-1.03);
- The Framework on Governance and Management of Information Resources of Public Bodies ;
- The *Directive on the security of government information* (C .T. , Decree 7-2014) ;
- The *Act to establish a legal framework for information technology* (LRQ, c. C-1.1)
- The *Criminal Code* (R.S.C., 1985, c. C-46)
- The *Regulation respecting the distribution of information and the protection of personal information* (c. A-2.1, r. 2)
- The *Directive sur la sécurité de l'information gouvernementale*;
- The *Copyright Act* (R.S.C., 1985, c. C-42)

4. SCOPE

This policy is intended for all users of information. This includes all personnel and is any natural or legal person who, as an employee, a trainee, a consultant, a volunteer, a partner, a supplier, a student, or a member of the public, uses the information assets of the school board.

The information referred to is that which ESSB holds in the course of its activities, whether it is maintained internally or by a third party; this includes digital and non-digital information.

5. DEFINITIONS

In this policy, the following words mean:

Information asset: A collection of information supported by a medium. The information is defined and structured, in a tangible or logical way according to the medium that carries it, and it is understandable in the form of words, sounds or images. The information may be created using any writing mode, including a system of symbols transcribed in one form or another.

It also includes any data bank whose organization allows for the creation of documents according to the restrictions and information structure that is stored therein.

Confidentiality: Principle that information is to be accessible only to designated and authorized persons or entities and be disclosed only to them.

Life Cycle of Information: All the stages that information goes through, from recording, transfer, consultation, processing and transmission to retention or destruction. All in accordance with the ESSB's retention schedule.

Availability: Informational property to be accessible in a timely manner and in the manner required by an authorized person.

Integrated Information Management: Management of all information produced or received by the school board, regardless of the medium they are on (print, technological, vocal and visual).

Information Security Incident: A harmful event, foreseeable or confirmed, that has consequences impacting the availability, integrity or confidentiality of the information. It may or may not be related to the use of information and communication technologies.

Confidential Information: Any information contained in a document held by the school board, in any medium whatsoever, the disclosure of which is not provided for in the *Act respecting access to documents held by public bodies and the protection of personal information, RSQ, c. A-21* and, in particular, the personal information held by the school board.

Integrity: Property associated with information not going through any alteration or destruction without authorization, and being kept on a support medium giving it stability and durability.

User: ESSB staff and any natural or legal person who, as an employee, consultant, volunteer, partner, supplier, student or member of the public, uses an information asset of the school board or has access to it, as well as any person duly authorized to have access to it.

6. SPECIFIC OBJECTIVES

1. To recognize the importance of information security;

2. To put security measures in place that are in proportion to the value of the information to be protected;

3. To ensure that authorized users have access to available, reliable, and confidential information throughout its lifecycle.

4. To ensure a good understanding of the information that needs protection, to identify the principal holders and their security features;

5. To design, plan, organize, develop and advance activities related to the creation, preservation, classification, processing, use, sharing, access, tracking and destruction of all documents required for the activities of the school board, regardless of the system and technology used;

6. To make users aware of sound management of information assets, including through training and awareness activities.

7. To recognize the increased risks of a computerized system of information management.

8. To focus on, through formal processes, risk management, access management and incident management.

7. ROLES AND RESPONSIBILITIES

7.1 The Council of Commissioners

Is responsible for the adoption and revision of this policy. It designates those responsible for LGGRI and DSIG.

7.2 The Administration Committee (AC)

Is responsible for the application of this policy in all administrative units of the school board.

7.3 The Secretary General

Assists the Director General in determining strategic directions and intervention priorities for integrated information management and privacy.

Develops, updates, and disseminates the management frameworks, directives, guides and procedures necessary for the security of non-digital information of the school board.

Provides the necessary support to departments and administrative units in the application of these documents and this policy.

7.4 The Information and Communications Technology Service

Assists the Director General in determining strategic directions and priorities for digital information security.

Develops, updates, and disseminates the management frameworks, directives, guides and procedures necessary for the security of the school board's digital information.

Ensures the necessary support to departments and administrative units in the application of these documents and this policy.

7.5 The Holder of the Information

Holders of the information must ensure the security of the confidential information of the school board placed at their disposal and at the disposal of persons under their authority. They must ensure that access to the confidential information of the school board is accessible only to those who require it for their activities.

7.6 Service Directors and Principals/Centre Administrators

The service directors and school/centre administrators are the holders of the information in their administrative unit. They are responsible for implementing the provisions of this policy with staff under their authority. To this end, they must:

a) Ensure that this policy is circulated to and understood by all members of their staff, as well as other management documents derived therefrom;

b) Ensure that this policy is respected in their administrative unit;

c) Sensitize their staff members to the security of the information assets to which they have access, the consequences of an attack on the security of information assets, as well as their roles and obligations in this regard;

d) Ensure the application of all management frameworks issued by the Secretary General and the Information Technology Department in connection with this policy;

e) Report any information security incident to the General Secretariat (non-digital information) or the Information and Communications Technology Service (digital information).

7.7 Users

Every user must:

a) Become acquainted with this policy and the resulting management frameworks, adhere to it and make a commitment to comply with it,

b) Use the information assets to which he/she has access in the course of his/her activities in accordance with this policy, as well as in accordance with laws, regulations, policies, procedures, directives and other administrative documents of the school board, in particular with respect to:
    a. The protection of personal information,
    b. Copyright and intellectual property.

c) Protect the information assets made available by using them judiciously, only for the intended purposes and within the accesses that are authorized to him/her;

d) Report, without delay, to his/her immediate superior any incident or anomaly of which he/she is aware that could constitute a real or presumed violation of the security rules, in particular:

    a. the theft or loss of confidential information,
    b. the intrusion into a network or a system, or
    c. any anomaly that may affect the protection of the information assets of the school board.

8. SANCTIONS

Any users who contravene this policy expose themselves to an intervention and/or disciplinary, administrative or legal measures.

9. ENTRY INTO FORCE

This policy comes into force on February 18, 2020, and remains in effect until repealed or replaced.