COMMISSION SCOLAIRE
Eastern Townships
SCHOOL BOARD

Moving ahead. Together. | Aller de l'avant. Ensemble.

SECURITY OF INFORMATION POLICY

Policy Name	Security of Information
Policy Number	P 041
Consultation Period	November 7th, 2022, to January 11th, 2023
Adopted Date by Council	April 26, 2023
Effective date	April 26, 2023
Source	Educational Services

TABLE OF CONTENTS

1. CONTEXT

The Act Respecting Governance and Management of the Information Resources of Public Bodies and Government Enterprises (*LGGRI*) (*LRQ*, Bill 133), enacted in 2011, and the Directive on the Security of Government Information (*DSIG*) (a directive from the Quebec Treasury Board and applicable to the school board), enacted in 2014, establishes obligations for educational institutions in their capacity as public bodies.

This policy allows the Eastern Townships School Board (ETSB) to carry out its mission, preserve its reputation, respect the laws and reduce risks while protecting the information it has created or received (of which it is the custodian). This information related to human resources, materials, technology and finances, is accessible in both digital and non-digital format, thus the dangers of a breach to its availability, integrity or confidentiality could have consequences linked to:

- The life, health or well-being of individuals;
- The breach of their personal information and of their private life;
- The provision of services to the population;
- The image of the ETSB and of the Government.

2. DEFINITIONS

Information asset

This term refers as much to the information contained in a document and to the system that supports it. The information asset may be comprised electronic documents, paper documents or even a database. It may also take the form of information technology, an installation, a computer asset or a combination of these elements.

Categorization of information assets

Recognizing that not all information at the Eastern Townships School Board is considered confidential in nature, the categorization of information assets in information security is a process that allows us to evaluate the degree of sensitivity of the information held by the ETSB in order to determine the level of protection regarding the potential risks of availability, integrity, confidentiality, authentication and irrevocability.

The ETSB can therefore consider the degree of sensitivity of its information assets in order to put into place the measures that will allow it to comply with its legal obligations, avoid financial losses, reach its objectives with respect to providing services and boost the confidence of citizens and businesses pertaining to its services and that of public services in general.

Thus, the categorization of an information asset serves as a basis for safeguarding the medium on which the information is kept (paper format, digital format, recording, audiovisual, etc.).

Information life cycle

The life cycle of information consists of all the steps the information passes through from its creation, by way of its recording, transfer, consultation, processing and transmission, until its conservation or destruction, in accordance with the ETSB retention schedule.

Document

This term describes a form of information found on a support medium. This information is defined and structured, in either a tangible or logical way depending on the medium, and is readable in the form of words, sounds or images. It can be transmitted by any means of writing, including a system of symbols transcribed in one of these forms. It is incorporated into a database whose structuring element allows for the creation and registration of documents through the defined and structured information entered.

Incident Management

The incident management process allows the organization to be prepared ahead to deal with incidents that could compromise information security, from the moment the incident occurs until things are back to normal. It provides, if necessary, an escalation to ministerial and governmental authorities. It also provides links to other processes of the ETSB, including local emergency measures.

Government Related Information Security Incidents

This term describes a visual consequence of an occurrence of a risk to government-related information. Concerted action at the government level is then necessary.

Rule

This general term includes the present policy, future management guidelines and directives as well as the applicable laws and regulations, in particular the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information and the Criminal Code.

Personal and Confidential Information

Section 54 of the Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (RLRQ, chapter A-2.1) states the following: *In any document, information concerning a natural person which allows the person to be identified is personal information.*

The Quebec Access to Information Commission has specified the three criteria enumerated in this article in order to establish whether information is personal or not:

- It must be *information* (the information makes something known);
- The information must *relate to* (be related to) a natural person;
- It must allow for the *identification* of this person (to recognize them in relation to another person or by different classes or categories of individuals or to also recognize their character).

Physical Security

Physical security includes protecting physical access to the sites, equipment, material, documents and people.

3. LEGAL AND ADMINISTRATIVE FRAMEWORK

The Information Security Policy is primarily part of a context governed by:

- The Charter of Human Rights and Freedoms (C.Q.L.R. chapter C-12);
- The Education Act (C.Q.L.R. c. l-13.3);
- Regulation respecting the retention schedule, payment, deposit and elimination of public archives (C.Q.L.R. c. A-21.1, r.1);
- The Civil Code of Quebec (LQ, 1991, chapter 64);
- The Act respecting 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 (LRQ, chapter G-1.03);
- The Act to establish a legal framework for information technology (LRQ, chapter C-1.1);
- The Act respecting Access to documents held by public bodies and the Protection of personal information (LRQ, chapter A-2.1);
- The Criminal Code (LRC, 1985, Chapter C-46);
- The Regulation respecting the distribution of information and the protection of personal information (RRQ, chapter A-2.1, r. 2);
- The Directive on the Security of Government Information;
- The Copyright Act (LRC, 1985, chapter C-42);
- The Archives Act (LRQ, A-21.1);
- The Policy on the use of Computer Resources.

4. SCOPE OF APPLICATION

The current policy is intended for information users, namely all personnel, regardless of their status and any natural or legal person whether student, parent, partner, consultant, supplier or visitor that uses or has access to the information assets of the ETSB as well as any other person duly authorized to access this information.

The information referred to is that which the ETSB possesses in the performance of its duties, whether its preservation is provided by itself or by a third party.

5. OBJECTIVE

The objective of this current policy is to affirm the ETSB's commitment to fully comply with its obligations with respect to the security of its information, regardless of the medium or means of communication. More specifically, the ETSB must ensure:

- The availability of the information in such a way that it is accessible in a timely manner and in the manner required by authorized persons;

- The integrity of the information in such a way that it is neither destroyed nor altered in any way without authorization, and that the medium for this information provides the desired stability and sustainability;

- The confidentiality of the information, by limiting the disclosure and use of it to authorized persons only, especially if it constitutes personal information.

For that reason, the ETSB will implement this policy in order to determine and direct its vision, which will be explained in the ETSB's Security of Information guidelines.

6. GENERAL GUIDELINES

The principles guiding the ETSB's actions regarding security of information are as follows:

a) To recognize the importance of the Security of Information Policy;

b) To fully understand the information that needs to be protected, by identifying the owners and their security levels;

c) To recognize that the technological environment of information assets is constantly changing and interconnected with the world;

d) To protect the life cycle of the information;

e) To ensure that each employee has access to the minimum amount of information required to accomplish their regular duties (essential);

f) Produce guidelines for users to define the correct use of the information assets;

g) To sensitize and train users about the security of information assets, the consequences of a breach of security as well as their roles and responsibilities in this matter.

7. ROLES AND RESPONSIBILITIES

Council of Commissioners

The Council of Commissioners will appoint a Chief of the Security of Organizational Information (CSOI), two Coordinators of Information Security Measures and will adopt the Information Security Policy as well as all amendments to it.

Chief of the Security of Organizational Information (CSOI)[1]

The Chief of the Security of Organizational Information for the ETSB is primarily responsible for the security of its information. For this reason, it complies with the government's information security guidelines and carries out its duties as issued by the Directive on the Security of Government Information. The CSOI will appoint a Cyber Defense Operations Manager (CDOM) and its substitute.

[1] The title and responsibilities of each representative may vary according to the directives of the Ministère de la cybersécurité et du numérique.

Organizational Incident Management Coordinator (OIMC)[1]

The two Organizational Incident Management Coordinators are appointed by the Council of Commissioners. These work closely with the CSOI to ensure the application of the government's information security guidelines. The main responsibilities are:

- To advise senior management on strategic guidelines;
- To ensure the coordination and coherence of the security of information (SI) guidelines undertaken by the ETSB and all its partners;
- To convey and coordinate the implementation of the processes;
- To oversee the rendering of accounts;
- To establish links with other information security officers.

Cyber Defense Operations Manager (CDOM)[1]

The CDOM provides support to the CSOI, notably with regards to the management of incidents and the risks to the information security. The main responsibilities are:

- To implement the Information Security (IS) processes;
- To contribute to the IS risk analysis (ex.: exposure to cyberattacks);
- To coordinate the management of a government-wide incident;
- To proceed with an automated assessment of the computer security system at the ETSB;
- To maintain a constant watch over potential risks, threats and vulnerabilities;
- To maintain a relationship with other SIMC coordinators.

Information Security Committee

The objective of the Information Security Committee is to assist the Chief of the Security of Organizational Information with the implementation of the Information Security Management Guidelines and any other elements that may be required to ensure the protection of the ETSB and to comply with the regulations.

Information Technology Department

The Information Technology Department is responsible for the development and maintenance of the tools that are consistent with the ETSB's information security objectives. They prepare development projects and/or implement system information acquisitions. They participate in risk analysis and anticipate threats to the information system's security. They take whatever measures are necessary to counter threats or any incident regarding information security. They participate in investigations relating to real or apparent contraventions to the current policy and as authorized by the Director General.

[1] The title and responsibilities of each representative may vary according to the directives of the Ministère de la cybersécurité et du numérique.

Material Resources Department

The Material Resources Department, along with the SIMC and ISO, participates in the identification of physical security measures that allow them to provide adequate protection for the ETSB's information assets.

Human Resources Department

With respect to information security, the Human Resources Department ensures that every ETSB employee is advised of the information security policy and procures their commitment with respect to the policy.

School Principals, Administrators and Centre Directors

As regards information security, School Principals, Administrators and Centre Directors ensure compliance with the policy, the management guidelines and the directives contained therein. They are the keepers of the information. Their role consists of ensuring the accessibility, the proper use of and the security of the information assets in their respective ETSB schools and centres and departments. They must:

- See to the protection of the information and the information systems under their responsibility and make sure that these are used by employees under their authority in accordance with the information security policy as well as all other elements of the management guidelines;

- Ensure that the information security requirements are considered in every acquisition process and every service contract under their responsibility and see that every consultant, supplier, partner, guest, organization or outside firm is committed to respecting the policy as well as all other elements of the management guidelines;

- Report all threats and incidents pertaining to information security to the CDOM;

- Collaborate in the implementation of any measure aimed at improving the information security, for repairing an information security breach as well as with every verification operation of the information assets security;

- Report any problem related to the implementation of the policy to the SIMC, including any real or perceived contravention by a staff member concerning the implementation of this policy.

Users

All users are obligated to protect the information assets made available to them as part of their duties. The information referred to is that which the ETSB holds as part of its activities, whether its conservation is ensured by itself or by a third party. Information assets can be found in digital or non-digital format. Therefore, every ETSB employee must:

a) Acknowledge, adhere to, and agree to comply with the current policy, directives, procedures and other guidelines contained therein, by signing the attached declaration;

b) Use the information assets at their disposal, within the right to access guidelines assigned to them and only when it is deemed necessary for carrying out their duties and limited to the purpose for which they are intended;

c) Comply with the security measures implemented on their workstation and on any equipment containing data that must be protected and to make no modifications to their configuration nor deactivate them;

d) Comply with the legal requirements concerning the use of products regarding any intellectual property rights that may exist;

e) Immediately notify their superior of any act that, to their knowledge, may constitute a real or alleged violation of the security regulations as well as any anomaly that could undermine the protection of the ETSB's information assets.

8. RIGHT OF REVIEW AND SANCTIONS

When a user violates the policy, whether in the management guidelines or the directives therein, they are liable to disciplinary, administrative or legal action, depending on the seriousness of their conduct.

The ETSB has a right of review over the use of their information assets by users, notably by controlling their right of access to said information. Hence, any expectation by the user regarding the protection of privacy is restricted.

Anyone who has broken a rule applying to the protection or security of information is, among other things, liable to one of the following sanctions:

- The cancellation of their right to use the information assets subject to the current policy;
- The reimbursement to the ETSB for any sum that the latter would be required to incur due to an unauthorized, fraudulent or illicit use of the information assets subject to the current policy;
- Staff members may be liable to administrative measures or disciplinary sanctions in accordance with collective agreements or regulations concerning terms of employment whether executive or non-executive as well as applicable laws;
- Students are liable to sanctions as set out in the centre's or school's code of conduct;
- Stakeholders, mandataries and suppliers are also liable to administrative measures, such as the termination of the contract or expulsion of the individual working on their behalf;
- Lastly, criminal or penal procedures could be taken against any individual who violates any one of these rules.

Exemption: The holder of the information who has a valid reason to not comply with a specific requirement or to not resort to a fixed security measure can ask for an exemption from the General Directorate after having carefully assessed the risks associated with this exemption.

9. ENFORCEMENT OF THE POLICY

The Director General is responsible, in collaboration with the Chief of Chief of the Security of Organizational Information (CSOI), for implementing this policy. The Organizational Incident Management Coordinators (OIMC) also contribute to its implementation.

10. COMMUNICATION OF THE POLICY

Chief of Chief of the Security of Organizational Information (CSOI), assisted by the Information Security Committee, of which at least one Organizational Incident Management Coordinator (OIMC) must be included, ensures the communication and updating of the policy.

11. EFFECTIVE DATE

The current policy came into effect on the date of its adoption by the Council of Commissioners, namely, on March 28, 2023.

COMMISSION SCOLAIRE
Eastern Townships
SCHOOL BOARD

ANNEX I

DECLARATION OF COMMITMENT BY EMPLOYEES CONCERNING THE INFORMATION SECURITY REGULATIONS

Users are obligated to protect the information assets made available to them by the ETSB. Therefore, they must:

- ✓ Comply with the ETSB's directives, in accordance with the Information Security Policy as well as all other procedures and guidelines relating to the ETSB's information security;
- ✓ Use the information assets within the right of access guidelines assigned to them and only when they are deemed necessary to carry out their duties and limited to the purpose for which they were intended;
- ✓ Comply with the security measures installed on their workstation and on any equipment containing data that must be protected and to make no modifications to their configuration nor deactivate them;
- ✓ Comply with the legal requirements concerning the use of products with regard to any intellectual property rights that may exist;
- ✓ Immediately notify their superior of any act that, to their knowledge, may constitute a real or alleged violation of the security regulations as well as any anomaly that could undermine the protection of the ETSB's information assets;
- ✓ At the time of their departure from the ETSB, return the various identity and access cards and the information assets as well as any computer or telephony equipment that was made available to them in order to carry out their duties.

I the undersigned, _____, acknowledge having read the regulations, as stated above, on the security information for the ETSB and agree to abide by them.

Signature: _____ Date: _____