Riverside School Board

Policy Name:	Policy on the Security of Information
Policy Number:	B734-20191217
Date Submitted to Executive:	October 1, 2019
Date received at Council:	October 15, 2019
Consultation Period:	October 18, 2019 – December 2, 2019
Date Approved by Council:	December 17, 2019

TABLE OF CONTENTS

1. CONTEXT

The Act Respecting the Governance and Management of the Information Resources of Public Bodies and Government Enterprises (AGMIR, LRQ, Bill 133) and the *Directive sur la sécurité de l'information gouvernementale* (DSIG, a directive of the Québec Treasury Board applicable to school boards) impose obligations on educational institutions in their capacity as public bodies.

The *Directive sur la sécurité de l'information gouvernementale* requires that school boards adopt, implement, update and enforce an information security policy—whose main provisions are set out in the government's directive—specifically through formal information security processes that make it possible to manage risks, access to information and incidents. This means that every school board must fulfill two roles by naming an information security manager (RSI) and two (2) sector coordinators for incident management (CSGI).

This policy enables Riverside School Board to achieve its missions, maintain its reputation, comply with legal requirements, and reduce risks while protecting the information it creates or receives (and for which it is responsible). This information pertaining to human, physical, technological and financial resources is accessible in digital and non-digital formats; risks threatening the accessibility, integrity and privacy of that information can have consequences that compromise:

- The life, health or wellbeing of individuals
- The protection of personal information and privacy
- The delivery of services to the public
- The image of the school board and of the government.

2. OBJECTIVES

The goal of this policy is to affirm the school board's commitment to fully discharge its obligations pertaining to the security of information, wherever it is stored and however it is communicated. More specifically, the school board is responsible for:

- The availability of information when and how authorized persons require it;
- The integrity of information such that it is neither destroyed nor altered in any way without authorization and that the medium used to store it provides the desired stability and sustainability;
- The privacy of information by limiting its disclosure and use to authorized persons, especially when it contains personal information.

The school board has therefore adopted this policy in order to orient and define its vision, which is detailed in the school board's management framework for information security.

3. LEGAL AND ADMINISTRATIVE FRAMEWORK

This security policy is governed primarily by the following:

- The *Charter of human rights and freedoms* (LRQ, c. C-12)
- The *Education Act* (LRQ, c. I-13.3)
- *Regulation respecting retention schedules, transfer, deposit and disposal of public archives* (LRQ, c. A-21.1, r.1)
- The *Civil Code of Québec* (LQ, 1991, c. 64)
- The *Policy Framework for the Governance and Management of the Information Resources of Public Bodies*
- The *Act respecting the governance and management of the information resources of public bodies and government enterprises* (LRQ, Bill 133)
- The *Act to establish a legal framework for information technology* (LRQ, c. C-1.1)
- The *Act respecting access to documents held by public bodies and the protection of personal information* (LRQ, c. A-2.1)
- 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)
- The Riverside School Board Use of technology Policy, February 16, 2010
- The Riverside School Board Safe, Respectful and Drug-free Environment in schools Policy, January 30, 2018
- The Riverside School Board Policy to Prevent and Address Harassment January 30, 2018

4. SCOPE OF APPLICATION

This policy is intended for information users, i.e. all staff and any natural or legal person who, as an employee, consultant, partner, supplier, student or member of the public, uses the school board's information assets. All users have an obligation to protect information assets made available to them by the school board. To this end, users must:

a) Be aware of this policy, as well as of any directives, procedures and other guidelines arising therefrom, comply with provisions therein, and undertake to do so by signing the attached declaration;

b) Use the information assets made available to them solely for the intended purposes, and this in accordance with assigned access rights and only when necessary to the performance of their duties;

c) Respect the security measures installed on their work station, and on any other equipment containing information that needs to be protected, and never modify their configuration or

deactivate them;

d) Comply with legal requirements governing the use of products for which intellectual property rights may exist;

e) Immediately report to their superior any act of which they become aware that may constitute a real or presumed violation of security regulations, as well as any problem that might threaten the security of the school board's information assets.

This refers to all information, digital and non-digital, that the school board holds in the context of its activities, whether storage of that information is managed by the school board or by a third party.

Please refer to the "Information Security Glossary" for a detailed list of roles and responsibilities.

5. GUIDING PRINCIPLES

The following guiding principles inform the school board's actions pertaining to information security:

a) Develop a full understanding of the information that needs to be protected,

b) Recognize the importance of the information security policy;

c) Understand that the technological environment for digital and non-digital information assets changes constantly and is interconnected with the world;

d) Protect information throughout its life cycle (creation, processing, destruction);

e) Ensure that employees have access only to information that is required to perform their normal duties;

f) The use of digital and non-digital information assets must be governed by a policy or directive that explains the appropriate procedure to follow and sets out what is permitted and what is not.

6. RISK MANAGEMENT

An up-to-date categorization of information assets serves to support risk analysis by identifying the value of the information to be protected.

Management of the risks associated with the security of digital and non-digital information falls within the school board's overall risk management process. Risks with governmental implications are covered by the *Directive sur la sécurité de l'information gouvernementale*. Risk analysis also includes the purchase, development and operation of information systems by specifying security measures to be implemented as part of the system's deployment in the school board environment.

The level of protection of information is determined by:

- The nature of the information and its importance
- The probability of an accident, error or malicious act to which the information is exposed
- The consequences should such a risk materialize
- The level of risk deemed acceptable by the school board.

7. INCIDENT MANAGEMENT

The school board adopts information security measures in order to ensure the continuity of its services. To that end, it implements measures needed to achieve the following goals:

- Limit the occurrence of information security incidents
- Properly manage such incidents in order to minimize the consequences and re-establish activities or operations

Information security incidents with governmental implications are to be reported to the MÉES in compliance with the *Directive sur la sécurité de l'information gouvernementale*.

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

8. DIRECTIVES

Plan to review each of the following directives according to a predetermined schedule and update them as required.

A. Access Management

The management of physical access needs to be planned, supervised and controlled in order to protect the availability, integrity and privacy of digital and non-digital information. This management must include the approval, revalidation and destruction of accesses, as well as the archiving of evidence of those management processes for future audits.

B. Vulnerability Management

The school board implements measures to keep its computer park up to date in order to minimize the vulnerability of its digital and non-digital information assets and reduce the probability of a cyber attack. Measures must be taken to warn of vulnerabilities originating with suppliers so that these can be corrected.

C. Backup Management

The school board must develop a backup strategy to guard against the loss of digital and non-digital information. This strategy must include keeping copies, error messages generated when

making copies, and copy restoration testing at appropriate intervals.

D. Business Continuity

The school board must develop a business continuity strategy in order to respond should an incident interrupt the delivery of a service. This strategy must be tested at appropriate intervals and any discrepancies corrected.

E. Protection of the Network Perimeter

The school board must plan penetration testing and vulnerability scanning to identify entry points that could allow inappropriate access to individuals or malware. Furthermore, a system to prevent and detect intrusions must be put in place to increase the level of protection. In addition, the school board can reduce the likelihood of a virus or attack spreading by segmenting its network.

F. Use of Personal Devices (B.Y.O.D.)

A directive on the use of personal devices (Tablets, smartphone, etc.) for performing one's duties must be developed to govern this practice, for it is essential that school board data be protected.

The parties must sign an agreement setting out their respective responsibilities and, in the event of the theft or loss of a device, authorizing the school board to erase its data on the missing device.

G. Protection of Non-Digital Information Assets

The school board must issue a directive on the protection of non-digital information assets primarily found in filing cabinets and printers. A culture of keeping offices orderly must be developed. These non-digital assets can be transported and produced in multiple copies. The notions of archiving and destruction must be taken into account in developing this directive. Protection measures should include managing physical access to rooms, printers and other areas where non-digital information assets are kept. The directive addressing perimeter protection should provide for intrusion testing, as well as for protective measures during the transit of information from one site to another.

H. Supplier Management

The school board must introduce a supplier management process to ensure that suppliers are not the source of incidents, the disclosure or loss of information, or viruses entering the network. To achieve this, an agreement must be signed stipulating that the supplier is committed to meeting the school board's cybersecurity requirements and that the school board is entitled to view the results of supplier audits (3416, SOC2, etc.). This agreement must also stipulate the objectives and level of service to be received from the supplier. Suppliers have access to sensitive school board information, and a confidentiality agreement must therefore be signed with each one in order to reduce the risk of disclosure of that information.

I. The Internet of Things (IOT)

The school board must put in place a process to oversee the IOT including tenfold cyber attack strike force of the type of a Distributed Denial of Services (DDOS), increase the surface of attack and personal data can be stored in a much more number of places.

9. AWARENESS RAISING AND TRAINING

Information security depends largely on regulating personal conduct and ensuring individual accountability. For this reason, the members of the school board community must be trained and made aware of:

- Information security and the school board's information systems
- Security directives
- Risk management
- Incident management
- Existing threats
- The consequences of a security breach
- Their role and responsibility in matters of security.

To this end, awareness-raising and training activities are organized periodically. In addition, explanatory documents are available on the school board's website.

10. SANCTIONS

Any school board employee who contravenes the legal framework, this policy or the information security measures resulting from it is subject to sanctions in accordance with the nature, severity and consequences of the contravention as prescribed by applicable law or internal disciplinary regulations (including those stipulated in collective agreements and the school board by-laws).

Suppliers, partners, guests, consultants and external organizations are subject to these sanctions.

11. POLICY DISTRIBUTION AND UPDATES

The RSI, with the support of the Information Security Working Committee, is responsible for distributing and updating this policy. The information security policy shall be reviewed periodically in accordance with updates made to it.

12. EFFECTIVE DATE

This policy came into effect on the date it was adopted by the Council of Commissioners, specifically on December 17, 2019.

INFORMATION SECURITY

GLOSSARY

Author:
André Bachand, SICS Project Director and Senior Advisor, Information Security

General Directorate of the “ABC” School Board
School Board Information Security Project (SICS)

HISTORY

Author	Role	Description	Date
André Bachand	Senior Advisor, IS	Creation	2017-11-28
André Bachand	Senior Advisor, IS	Modifications to the definitions of: accountability, confidential information, CSGI, information holder, information security measure, RSI security incident with government implications, Deletion of the definition of: information asset manager	2018-03-20

Table of Contents

Accountability

The principle by which an action/activity can be unequivocally attributed to the entity responsible (non-repudiation).

Authentication

Used to confirm the identity of a person or to identify a document or device.

Authority register

The directory, log or file in which the assignments and delegations of authority for the purpose of managing information security, as well as the associated responsibilities, are officially recorded.

Authorization

Assignment by the school board to an individual or group of the right to access, in whole or in part, specific information or an information system.

Availability

The property of information of being available when and how it is required by an authorized user.

Categorization

The process of assigning a value to certain characteristics of information so as to qualify its degree of sensitivity in terms of availability, integrity and confidentiality, and, consequently, the appropriate level of protection required.

Compensatory measure

A concrete measure that serves to reduce the probability of a risk materializing due to noncompliance.

Confidential information

Information whose access is subject to one or more restrictions set out in the *Act respecting Access to documents held by public bodies and the Protection of personal information* and the *Privacy Act*

and requires the consent of the information holder before being disclosed to anyone.

Confidentiality

The property of information by which it is to be available and disclosed only to designated and authorized persons or entities.

Continuity plan

All planning measures identified and implemented for the purpose of re-establishing the availability of information that is vital to conducting a school board activity.

Digital information asset

Any information stored in digital form on one of the following media: disk, database, diskette, magnetic tape, cassette, USB key, flash drive, video, digital photograph, laptop, desktop, tablet, smartphone, etc. The information on the digital media asset may be written, erased, rewritten, encrypted or copied.

Document

A set of information stored on a medium. The information is delimited and structured, tangibly or logically depending on the support medium, and intelligible in the form of words, sounds or images. The information may be rendered through any written means, including a system of symbols transcribed into an intelligible form or into another system of symbols. The notion of document includes any database whose structure can be used to create documents by delimiting and structuring the information it contains.

Duplicate entry for Information holder

Exemption

A form that has been completed and duly approved by the appropriate stakeholders authorizing an exception to a security requirement for a specified period of time after the risk, impact and any compensatory measures have been identified.

General Director

The General Director has overall responsibility for information security. See the nomination guide for more information.

General Secretary

General secretaries validate and approve IS policies. They prepare resolutions pertaining to nominations and policies and ensure compliance with the legislative framework.

Holder

An individual who has custody of part or all of one or more of the school board's information assets.

Human Resources Department

With respect to information security, the Human Resources Department ensures that all new employees of the school board are notified of the information security policy and that they agree to comply with the policy.

Incident

An event that jeopardizes or threatens to jeopardize the availability, integrity or confidentiality of information or, more generally, the security of information systems, especially by interrupting operations or reducing the quality of services.

Incident register

A log in which the nature of an information security incident, its impact, the underlying problem, and the measures taken to re-establish normal operations are recorded.

Information

Some kind of data recorded on a medium for the purpose of being stored, processed or communicated as an element of knowledge.

Information asset

Any asset containing digital or non-digital information, such as a database on a server or a paper document in a filing cabinet.

A piece or bank of information, an information system or medium, a document, an information technology or equipment, or a combination of any of the preceding, acquired or constituted by the school board that may be accessible with an information technology device (application, software package, educational software, database or information bank of textual, audio, symbolic or visual information stored on equipment or on an information medium, electronic mail system or voicemail system) or by a more traditional means such as a folder or filing cabinet. This includes information as well as tangible and intangible media used to process, transmit or store information for its intended purpose (computers, laptops, electronic tablets, smartphones, etc.), as well as information fixed on an analog medium such as paper.

Information holder

The information holder is the manager in the educational or administrative department authorized to oversee the accessibility, proper use and security of information assets for which their department is responsible. Consequently, there may be several information holders within a school board. They may delegate some or all of their responsibility to another member of the department. Information holders:

- Inform staff under their authority and third parties with whom the department deals of the information security policy and of provisions in the management framework so that they are aware of the need for compliance
- Collaborate actively in categorizing departmental information for which they are responsible and in analyzing risks
- Ensure the protection of information and information systems under their responsibility, and

further ensure that these are used by staff under their authority in compliance with the information security policy and any other provision in the management framework

- Ensure that information security requirements are taken into account in all purchasing processes and in every service contract under their responsibility, and further ensure that all consultants, suppliers, partners, guests, organizations and external firms agree to respect the information security policy and all the provisions in the management framework
- Report to the CSGI any threat to or incident involving the security of digital or non-digital information
- Collaborate in implementing any measure intended to improve information security or to remedy an information security incident, as well as any operation to verify the security of information assets
- Report to the CSGI any problem related to the application of the information security policy, including any real or apparent infraction by a staff member pertaining to the application of the information security policy

Information life cycle

All of the steps information goes through from creation—including recording, transfer, consultation, processing and transmission—until permanent storage or destruction in compliance with the school board's retention schedule.

Information security

The protection of information and information systems against risks and incidents.

Information security manager (RSI)

Person appointed by the Council of Commissioners to assume the position. The RSI has a strategic role and a relationship with senior management. He or she communicates to the school board orientations and priorities pertaining to information security and ensures that all school board stakeholders are on board and involved. See the nomination guide for more information.

Information security measure

A concrete means of ensuring the partial or total protection of the school board's information against one or more risks (major breakdown of the computer network or institutional servers, involuntary act, malicious act such as an intrusion into the computer system, disclosure or theft of documents, etc.) whose implementation is intended to reduce the probability of these risks materializing or to minimize the resulting losses.

Information security risk

The degree to which information or an information system is exposed to the threat of an interruption of or reduction in the quality of services, or a breach of the availability, integrity or confidentiality of information that may have consequences on any of the following: the delivery of services; the life, health or wellbeing of individuals; the respect of their fundamental rights to the protection of personal information and privacy; or the school board's image.

Information security risk with governmental implications

A threat to the availability, integrity or confidentiality of government information that could have consequences on the delivery of public services; the life, health or wellbeing of individuals; the respect of their fundamental rights to the protection of personal information and privacy; the image of the government; or the delivery of services provided by other public organizations.

Information system

All organized means put in place to collect, store, process, communicate, protect or delete information in order to meet a specific need, specifically including applications, software and software packages, information technologies and the procedures used to carry out these functions.

Information technology

Any software or electronic equipment, or combination thereof, used to collect, store, process, communicate, protect or delete information in any form (text, symbol, audio or visual).

Information Technology Department

In matters of information security, the Information Technology Department is in charge of information security requirements with respect to the operation of information systems, as well as in projects to develop or acquire information systems. Specifically, the Department:

- Participates actively in analyzing risks, evaluating needs and measures to be implemented, and anticipating any security threats to information systems using information technologies
- Takes appropriate measures to respond to any information security threat or incident, e.g. the temporary interruption or revocation, when circumstances so require, of the services of an information system using information technologies in order to ensure the security of the information concerned
- Participates in conducting inquiries authorized by the General Director into real or apparent contraventions of the information security policy.

Integrity

The property of information by which it is never altered or destroyed without authorization or accidentally and is stored on a medium and preserved using means that ensure its stability and sustainability. Integrity refers to the accuracy and completeness of information.

Management framework

All of the components—policies, regulations, directives, procedures, recognized best practices or committees—that provide a framework for the school board's activities.

Material Resources Department

Together with the CSGI/RSI, the Material Resources Department participates in identifying traditional risks and physical security measures that will adequately protect the school board's non-digital information assets.

Non-digital information asset

Any information in a format other than digital, including paper, microfilm, film, printed photograph, etc.

- Once information has been produced on a non-digital media asset, it can no longer be erased, rewritten, encrypted or copied.
- Non-digital assets can be found in a room, on a wall, in a filing cabinet, in a briefcase, in a backpack.
- Non-digital assets can be easily transported.
- They can be produced in multiple copies and stored in more than one place.
- Keeping track of non-digital information assets is challenging.
- A non-digital asset that has been digitized is still deemed to be a non-digital asset.
- Non-digital information can vary from one copy to another. E.g., a student's IEP may be digitized at the outset and then digitized a second time once all the professionals involved have signed it.
-

Personal information

Information concerning a physical person that can be used to identify that person. Personal information of a public nature under law is not considered personal information for the purposes of the information security policy.

Recovery plan

The offsite restoration plan to be implemented when information assets deteriorate or are destroyed because of an incident requiring the transfer of operations to another place. The recovery plan describes the procedures designed to ensure, under conditions of continuity in line with the school board's survival criteria, the rapid and orderly application of relief measures, as well as the eventual restoration of normal operations once the damaged or destroyed assets have been repaired or replaced.

Sector coordinator for incident management (CSGI)

Individual appointed by the Council of Commissioners to assume the position. Working in close collaboration with the MÉES OCIM-Network, the school board's CSGI is responsible for tactical and operational actions. He or she provides the support the RSI requires to discharge their responsibilities and is the organization's official contact person for CERT/AQ. See the nomination guide for more information.

Security incident with governmental implications

The observable consequence of the materialization of an information security risk that could affect government operations by jeopardizing the availability, integrity or confidentiality of information and thereby negatively impact the life, health or wellbeing of individuals; the protection of personal information and privacy; the delivery of public services; or the image of the school board and government, and so require a harmonized response at the government level.

Traceability

Traceability refers to a situation in which sufficient information exists to know (possibly in retrospect) the content of an asset throughout the production, transformation and distribution chain, whatever the location, from the origin of the product to the end of its life cycle.

User

Any individual, employee, parent or other physical person who uses a digital or non-digital network to access information held by the school board for the purposes of carrying out its mission. School board staff and students are the primary users of school board information. All users of school board networks must comply with policies and directives in effect in a business or organization with which they are associated in the context of their professional activities or studies when they share information assets, information technology devices or information systems.

Security evaluation criteria for digital and non-digital information (for documents in any form)

Availability

The property of information of being available when and how it is required by an authorized user.

Integrity

The property of information by which it is never altered or destroyed without authorization or accidentally and is stored on a medium and preserved using means that ensure its stability and sustainability. Integrity refers to the accuracy and completeness of information.

Confidentiality

The property of information by which it is to be available and disclosed only to designated and authorized persons or entities