Commission scolaire English-Montréal
English Montreal School Board

POLICY: INFORMATION SECURITY	CODE: ETS-18

Origin: **Educational and Technology Services**

Authority: **Resolution # 19-06-12-11.1**

References: **Refer to the Legal Framework**

NOTE: The masculine gender, when used in this document, refers to both women and men. No discrimination is intended.

1. POLICY STATEMENT

The Act Respecting the Governance and Management of the Information Resources of Public Bodies and Government Enterprises (AGMIR, LRQ, and Law 135) and the *Directive sur la sécurité de l'information gouvernementale* (DSIG, a directive of the Quebec Treasury Board applicable to school boards) imposes 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, determine and control access to information as well as prevent, track and recover from adverse events. To this end, the EMSB must name an employee responsible for Information Security (RSI) and a coordinator for incident management (CSGI) who will supervise the implementation and management of the Information Security Policy, hereafter known as the "Policy".

The EMSB:

1. recognizes the importance and legal responsibilities attached to the Information Security Policy;
2. ensures that the use of digital and non-digital information assets is governed by the Policy, and its associated practices and protocols that detail the appropriate procedures to follow throughout the life cycle of the information asset;
3. ensures that the Policy is aligned with EMSB risk management practices and protocols;
4. ensures that the Policy is aligned with adverse events practices and protocols to ensure recovery, return to continuity of services, user confidence and stability;
5. uses the Policy to achieve its mission, maintain its reputation, comply with legal requirements and reduce risks while protecting the information it creates, communicates and receives, and for which it is responsible, wherever and however it is stored and or communicated.

This information pertains to digital and non-digital resources and work products, be they proprietary or third-party.

The risks pertain to threats regarding the accessibility to, the integrity and privacy of information which can have consequences that compromise:

a) the life, health and well-being of individuals;
b) the protection of personal information and privacy;
c) the delivery of services;
d) the reputation of the EMSB and the government.

2. FIELD OF APPLICATION

This Policy applies at all times to all EMSB stakeholders – employees, youth and the adult and vocational sector students, commissioners, consultants, parents, partners, volunteers, suppliers and vendors – who access and or use EMSB information assets, regardless of the storage format, the means used to create, access and or communicate the information, the location from which the information is accessed, saved and or transmitted, and whether or not the information is managed or owned by the EMSB or a third party.

All stakeholders have an obligation to protect the EMSB's information assets made available to them by the EMSB or which they create, disseminate, archive or conserve on the EMSB network and or using EMSB assets. Therefore, stakeholders must:

a) be aware of the Policy, as well as any directives, procedures, protocols and other guidelines arising from the Policy including updates to the Policy;

b) comply with all applicable provisions of the Policy;

c) use the EMSB information assets made available to them solely for their intended purposes, in accordance with the stakeholder's assigned security level and profile for information rights, and only when required in the performance of their duties;

d) respect the security measures installed on the work devices and media they use;

e) comply with legal requirements governing the use of products for which intellectual property rights and or copyrights exist;

f) immediately report to their superior and to the RSI (via ITSecurity@emsb.qc.ca) any act of which they become aware that may constitute a real or presumed violation of the Policy, as well as any problem that may threaten the security of the EMSB's information assets.

3. LEGAL FRAMEWORK

a) *The Charter of human rights and freedoms (LRQ, c. C-12)*
b) *The Education Act (LRQ, c. I-13.3)*
c) *Regulation respecting retention schedules, transfer, deposit and disposal of public archives (LRQ, c. A-21.1, r.1)*
d) *The Civil Code of Quebec (LQ, 1991, c. 64)*
e) *The Policy Framework for the Governance and Management of the Information Resources of Public Bodies*
f) *The Act respecting the governance and management of the information resources of public bodies and government enterprises (LRQ, Law 135)*
g) *The Act to establish a legal framework for information technology (LRQ, c. C-1.1)*
h) *The Act respecting access to documents held by public bodies and the protection of personal information (LRQ, c. A-2.1)*
i) *The Criminal Code (R.S.C., 1985, c. C-46)*
j) *The Regulation respecting the distribution of information and the protection of personal information (c. A-2.1, r. 2)*
k) *The Directive sur la sécurité de l'information gouvernementale*
l) *The Copyright Act (R.S.C., 1985, c. C-42)*
m) *EMSB Records Retention Policy (SG-05)*
n) *EMSB Policy, Bill 65 – Access to documents and protection of personal information (SG-04)*
o) *EMSB Policy, Information and Communication Technologies – Access and Appropriate Use (DG-25)*
p) *EMSB schools' and centres' Codes of Conduct*
q) *EMSB Policy – Oath of confidentiality by observers from the EMSB's consultative groups*
r) *EMSB Policy on Video Surveillance (SG-11)*
s) *EMSB Policy – To Facilitate the Disclosure of Wrongdoings (DG-26.1)*
t) *EMSB Policy - Code of Ethics (HR-11)*
u) *EMSB By-Law No. 3 - Code of Ethics and Professional Conduct for Members of the Council of Commissioners*

4. OBJECTIVES

4.1 The EMSB:

a) develops a full, fluid and flexible understanding of the information that must be accessed and protected as per the changing technological, legal and ethical environments of information security, privacy and the school board;

b) identifies the holders and users of information and manages their security profile when and if their employment or student status changes, as per the information assets they require access to, in order to perform their normal work duties;

c) protects information throughout its life cycle – creation, processing, availability, integrity, use, storage / archiving, destruction, regardless of its format and access pathway;

d) regularly reviews and updates as necessary, the following practices and protocols:
   i. access management;
   ii. vulnerability management – warnings / alerts, preventative measures, testing;
   iii. back-up of information management;
   iv. business continuity – recovery and return to service measures;
   v. exposure to threats or incidents of system breaches, denials of service and or illegal activities;
   vi. awareness, training and monitoring of practices and protocols regarding the Policy;
   vii. communication to victims of an incident regarding the protection of confidential information;

e) provides access to information and oversight as to how authorized persons use and store the information;

f) maintains the integrity of the information such that it is neither destroyed nor altered in any way without authorization;

g) ensures that the format used to store the information provides and maintains its stability, sustainability, integrity, privacy and accessibility;

h) secures the privacy of the information by limiting its disclosure and use to authorized persons in the performance of their work duties.

4.2 The Human Resources department ensures that all new and existing employees of the EMSB are informed of the Policy and that they agree to comply with the Policy.

5. SANCTIONS

Any school board stakeholder – employee, youth, adult and vocational sector student, commissioner, consultant, parent, partner, volunteer, supplier and or vendor – who accesses and or uses EMSB information assets and 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 EMSB by-laws and policies).

6. DEFINITIONS

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

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

Adverse Event
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.

Adverse Event Register
A log in which the nature of the adverse event, its impact, the underlying problem, and the measures taken to re-establish normal operations and prevent a re-occurrence is recorded.

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 and access rights required.

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 that requires the consent of the information holder or owner before being disclosed to anyone.

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

Continuity Plan
All planning measures identified and implemented for the purpose of re-establishing the availability and integrity of the information that is vital to conducting an EMSB activity.

CSGI - Sector Coordinator for Incident Management
Individual appointed by the Council of Commissioners responsible for tactical and operational actions emanating from the Policy. The individual collaborates with the MEES OCIM-Network (Information Security Incident Management, for the education and higher education networks), provides support to the RSI and is the official contact person for CERT/AQ (Computer Emergency Response Team/Administration québécoise).

Information Asset
Any tangible item containing information in digital or analog (such as paper based) form and or the system or equipment used to store that information, acquired or constituted by the EMSB, accessible by a digital or analog device or tool, used to create, communicate, process, transmit or store the information.

Information Holder
A person in each EMSB department, school and centre responsible for, and authorized to, oversee the accessibility to, and the appropriate security of information practices and protocols for the information assets within the department, school and centre. Each department, school or centre may choose to name a person or persons to the role of Information Holder.

Information Holders:

1. Inform staff under their authority and third parties with whom the department deals, of the information security Policy and of provisions in the Procedural Guide so that they are aware of the need for compliance;

2. Collaborate with the RSI in:
   a. categorizing departmental and or school-based information for which they are responsible and in;
   b. analyzing potential risks.

3. 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 Procedural Guide;

4. Ensure that information security requirements are accounted for 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 Policy and all the provisions in the Procedural Guide. This will include the signing of a non-disclosure or confidentiality agreement, when appropriate;

5. Report to the CSGI (ITSecurity@emsb.qc.ca) any threat or incident pertaining to information security;

6. 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 digital or non-digital information assets;

7. Report to the RSI (ITSecurity@emsb.qc.ca) any problem related to the application of this Policy, including any real or apparent contravention by a staff member pertaining to the application of the Policy.

Information Life Cycle
All of the steps information goes through from creation to destruction, including recording, transfer, consultation, processing, communication, storage, archiving, until permanent storage or destruction according to the EMSB Records Retention Policy.

Information Security
The protection of information and information systems against adverse events and risks.

Information Security Measure
A concrete means to ensure protection of EMSB's information against risk and whose implementation is intended to reduce the probability of risks materializing, or to minimize the effects of an adverse event.

Information Security Risk
The degree to which information or an information system is exposed to the threat of an interruption or reduction of the quality of services, or a breach of availability, integrity or confidentiality of information.

Integrity
The property of information by which it is never altered or destroyed without authorization or accidentally, and is stored and preserved in a format that ensures its stability and sustainability. Integrity also refers to the accuracy and completeness of the information.

Non-digital Information Asset
Any information in a format other than digital such as paper, microfilm, film, printed pictures etc. These can be found in filing cabinets, drawers, briefcases, backpacks, on desks, in photocopier machines or printers etc. A non-digital information asset that has been digitized is still considered to be a non-digital information asset.

Personal Information
Information concerning a physical person which 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 Policy.

Recovery Plan
Procedures designed to ensure the rapid and orderly application of relief measures leading to the restoration of normal operations following an adverse event. The primary copy of the recovery plan and its components should be stored offsite.

RSI - Information Security Manager
Person appointed by the Council of Commissioners who communicates to EMSB stakeholders, regarding the orientations and priorities pertaining to information security.

Traceability
Situation in which sufficient information exists to know, possibly in retrospect, the contents of an information asset throughout its production, transformation and distribution chain, whatever the location, from the origin of the asset to the end of its life cycle.