Commission scolaire English-Montréal
English Montreal School Board

POLITIQUE : POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION	CODE : ETS-18
Origine : Services éducatifs et de la technologie	
Autorité : Résolution nº 19-06-12-11.1	
Références : Se référer au cadre juridique	

N. B. : Le générique masculin est utilisé dans ce document sans aucune discrimination et dans le seul but d'alléger le texte.

1. ÉNONCÉ DE POLITIQUE

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI) (LRQ, loi 135) et la Directive sur la sécurité de l'information gouvernementale (DSIG) (une directive du Secrétariat du Conseil du trésor applicable aux commissions scolaires) imposent des obligations aux établissements d'enseignement en leur qualité d'organismes publics.

Ainsi, la DSIG oblige la commission scolaire à adopter, à mettre en œuvre, à tenir à jour et à appliquer une politique sur la sécurité de l'information – dont les principales modalités sont définies dans la directive – en ayant spécifiquement recours à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la détermination et le contrôle de l'accès à l'information, et la prévention, la surveillance et la résolution des incidents. À cette fin, la CSEM doit désigner un responsable de la sécurité de l'information (RSI) et un coordonnateur sectoriel en gestion des incidents (CSGI) chargés de superviser la mise en œuvre et la gestion de la Politique sur la sécurité de l'information, ci-après appelée « la Politique ».

La CSEM :

1. reconnaît l'importance et les responsabilités légales liées à la Politique sur la sécurité de l'information;
2. s'assure que l'utilisation des actifs informationnels numériques et non numériques est conforme à la Politique, et aux pratiques et protocoles qui y sont liés établissant les procédures à suivre tout au long du cycle de vie de l'information;
3. veille à ce que la Politique soit cohérente avec les pratiques et protocoles de gestion des risques de la CSEM;
4. veille à ce que la Politique soit cohérente avec les pratiques et protocoles relatifs aux incidents liés à la sécurité pour assurer le rétablissement à la normale, le retour à la continuité des services, la confiance de l'utilisateur et la stabilité;
5. utilise la Politique pour réaliser sa mission, préserver sa réputation, observer les obligations légales et réduire les risques tout en protégeant l'information qu'elle crée, communique et reçoit et dont elle est responsable, sans égard au mode de conservation ou de communication.

L'information visée est celle que la commission scolaire détient sous forme de ressources et de produits du travail numériques ou non numériques, qu'elle soit sa propriété ou celle d'un tiers, et dont les risques d'atteinte à sa disponibilité, à son intégrité et à sa confidentialité peuvent avoir des conséquences liées à :

a) la vie, la santé et le bien-être des personnes;
b) la protection des renseignements personnels et de la vie privée;
c) la prestation de services;
d) l'image de la CSEM et du gouvernement.

2. CHAMP D'APPLICATION

La Politique s'applique en tout temps à chaque intervenant de la CSEM – employé, élève du secteur des jeunes, des adultes et de la formation professionnelle, commissaire, consultant, parent, partenaire, bénévole et fournisseur – qui a accès aux actifs informationnels de la CSEM ou les utilise, sans égard au format de stockage, au moyen utilisé pour créer l'information, y accéder et la transmettre, au lieu à partir duquel il accède à l'information, la sauvegarde ou la transmet, au fait que l'information soit détenue et gérée par la CSEM ou par un tiers.

Tout utilisateur a l'obligation de protéger les actifs informationnels de la CSEM mis à sa disposition par la CSEM ou qu'il crée, transmet, archive ou conserve sur le réseau de la CSEM. À cette fin, il doit :

a) prendre connaissance de la Politique, des directives, des procédures, des protocoles et des autres lignes de conduite en découlant, y compris les mises à jour à la Politique;

b) se conformer à toutes les dispositions applicables de la Politique;

c) utiliser, conformément à sa cote de sécurité, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels de la CSEM mis à sa disposition en se limitant aux fins auxquelles ils sont destinés;

d) respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données qu'il utilise;

e) se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle et/ou des droits d'auteur existent;

f) signaler immédiatement à son supérieur et au RSI (à ITSecurity@emsb.qc.ca) tout acte dont il a connaissance susceptible de constituer une violation réelle ou présumée de la Politique ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la CSEM.

3. CADRE JURIDIQUE

a) Charte des droits et libertés de la personne (LRQ, c. C-12)
b) Loi sur l'instruction publique (LRQ, c. I-13.3)
c) Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (LRQ, c. A-21.1, r.1)
d) Code civil du Québec (LQ, 1991, c. 64)
e) Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics
f) Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, loi 135)
g) Loi concernant le cadre juridique des technologies d'information (LRQ, c. C-1.1)
h) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, c. A-2.1)
i) Code criminel (L.R.C. (1985), c. C-46)
j) Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (c. A-2.1, r. 2)
k) Directive sur la sécurité de l'information gouvernementale
l) Loi sur le droit d'auteur (L.R.C. (1985), c. C-42)
m) Politique de la CSEM - Conservation de documents (SG-05)
n) Politique de la CSEM - Loi 65 - Accès aux documents et protection de l'information personnelle (SG-04)
o) Politique de la CSEM - Technologie de l'information et des communications - Accès et utilisation appropriée (DG-25)
p) Codes de conduite des écoles et des centres de la CSEM
q) Politique de la CSEM - Serment de confidentialité des observateurs des groupes consultatifs de la commission (SG-03)
r) Politique sur la vidéosurveillance à la CSEM (SG-11)
s) Politique de la CSEM - Politique visant à faciliter la divulgation d'actes répréhensibles (DG-26.1)
t) Politique de la CSEM - Code d'éthique (HR-11)
u) Règlement n^{o} 3 de la CSEM - Code d'éthique et de déontologie des membres du conseil des commissaires

4. OBJECTIFS

4.1 La CSEM :

a) acquiert une compréhension complète, fluide et souple de l'information qui doit être utilisée et protégée en fonction de l'environnement technologique, légal et éthique en changement constant de la sécurité de l'information, de la vie privée et de la commission scolaire;

b) identifie les détenteurs et les utilisateurs de l'information et gère leurs cote de sécurité et droits d'accès lorsque leur statut d'emploi ou d'élève change, en fonction des actifs informationnels auxquels ils doivent accéder dans l'exercice de leurs fonctions;

c) protège l'information tout au long de son cycle de vie – création, traitement, disponibilité, intégrité, utilisation, stockage/archivage, destruction, sans égard au format de l'information ou à son mode d'accès;

d) examine sur une base régulière et met à jour au besoin les pratiques et protocoles suivants :
   i. gestion de l'accès;
   ii. gestion de la vulnérabilité – avertissements/alertes, mesures préventives, tests;
   iii. gestion de la sauvegarde de l'information;
   iv. continuité des services – mesures de rétablissement et de retour à la continuité des services;
   v. exposition aux risques et aux incidents d'intrusion, d'interruption de services et d'activités illégales;
   vi. sensibilisation, formation et suivi quant aux pratiques et aux protocoles liés à la Politique;
   vii. communication aux victimes d'un incident lié à la protection de renseignements confidentiels;

e) donne accès à l'information et exerce une surveillance relativement à l'utilisation et au stockage de l'information par les personnes autorisées;

f) préserve l'intégrité de l'information de sorte que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation;

g) veille à ce que le support utilisé pour conserver l'information assure et préserve sa stabilité, sa durabilité, son intégrité, son caractère confidentiel et son accessibilité;

h) assure la confidentialité de l'information en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées dans l'exercice de leurs fonctions.

4.2 Le Service des ressources humaines veille à ce que tous les employés de la CSEM, nouveaux et actuels, soient mis au courant de la Politique et acceptent de s'y conformer.

5. SANCTIONS

Tout intervenant de la CSEM – employé, élève du secteur des jeunes, des adultes et de la formation professionnelle, commissaire, consultant, parent, partenaire, bénévole et fournisseur – qui a accès aux actifs informationnels de la CSEM ou les utilise et qui contrevient au cadre légal, à la présente Politique ou aux mesures de sécurité de l'information en découlant s'expose à des sanctions selon la nature, la gravité et les conséquences de l'infraction, conformément à la loi ou aux règlements disciplinaires internes applicables (y compris ceux énoncés dans les conventions collectives et les règlements et politiques de la CSEM).

6. DÉFINITIONS

Registre d'autorisation
Répertoire ou fichier dans lequel sont officiellement consignées les attributions et délégations d'autorisation et de droits d'accès aux fins de la gestion de la sécurité de l'information, ainsi que les responsabilités qui y sont liées.

Autorisation
Attribution par la CSEM à une personne ou à un groupe du droit d'accès, en tout ou en partie, à de l'information ou à un système d'information spécifique.

Incident
Événement qui porte atteinte ou peut porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information ou, de façon plus générale, à la sécurité des systèmes d'information, surtout en entraînant une interruption ou une détérioration de la qualité des services.

Registre d'incident
Recueil dans lequel sont consignés la nature de l'incident, l'impact, le problème sous-jacent et les mesures prises pour le rétablissement à la normale et la prévention d'un nouvel incident.

Catégorisation
Processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information en termes de disponibilité, d'intégrité et de confidentialité et, conséquemment, le degré de protection et de droits d'accès requis.

Renseignement confidentiel
Renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels* et qui exige le consentement du détenteur de l'information pour toute divulgation.

Confidentialité
Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Plan de continuité
Ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité et l'intégrité de l'information indispensable à la réalisation d'une activité de la CSEM.

CSGI – Coordonnateur sectoriel en gestion des incidents
Personne nommée par le conseil des commissaires responsable des mesures tactiques et opérationnelles découlant de la Politique qui collabore avec le réseau OCIM du MEES (gestion des incidents de sécurité de l'information pour les réseaux de l'éducation et de l'enseignement supérieur), apporte son soutien au RSI et agit à titre de contact officiel pour le CERT/AQ (équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise).

Actif informationnel
Information, quels que soient son canal de communication (numérique ou analogique) ou son support (papier ou autre), système ou support d'information, acquis ou constitués par la CSEM, accessibles au moyen d'un appareil ou d'un outil numérique ou analogique, utilisés pour créer, communiquer, traiter, transmettre ou stocker l'information.

Détenteur de l'information
Personne désignée au sein de chaque service, école et centre de la CSEM qui a le rôle et l'autorisation de s'assurer de l'accessibilité et de la sécurité des pratiques et des protocoles pour les actifs informationnels relevant de la responsabilité de son unité administrative. Chaque service, école ou centre peut désigner comme détenteur de l'information une ou plusieurs personnes.

Le détenteur de l'information :

1. s'assure que le personnel relevant de son autorité et les tiers avec lesquels transige son unité administrative sont au fait de la Politique sur la sécurité de l'information et des éléments du guide de procédures et s'engagent à s'y conformer;

2. collabore avec le RSI en :
   a. catégorisant l'information de l'unité administrative ou de l'école dont il est responsable;
   b. analysant les risques potentiels.

3. voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la Politique sur la sécurité de l'information et tout autre élément du guide de procédures;

4. s'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité, et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la Politique et tout autre élément du guide de procédures, notamment en signant au besoin une entente de non-divulgation ou de confidentialité;

5. signale au CSGI (à ITSecurity@emsb.qc.ca) toute menace ou tout incident afférant à la sécurité de l'information;

6. collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information, ainsi qu'à toute opération de vérification de la sécurité des actifs informationnels numériques ou non numériques;

7. signale au RSI (à ITSecurity@emsb.qc.ca) tout problème lié à l'application de la Politique, dont toute infraction réelle ou apparente d'un membre du personnel en qui a trait à l'application de la Politique.

Cycle de vie de l'information
Ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement, sa transmission, son stockage et son archivage, jusqu'à sa conservation permanente ou sa destruction, en conformité avec la Politique sur la conservation de documents de la CSEM.

Sécurité de l'information
Protection de l'information et des systèmes d'information contre les incidents et les risques.

Mesure de sécurité de l'information
Moyen concret assurant la protection des actifs informationnels de la CSEM contre les risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

Risque de sécurité de l'information
Mesure selon laquelle une information ou un système d'information est exposé à la menace d'interruption et de réduction de la qualité des services, ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information.

Intégrité
Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation ou par inadvertance, et d'être conservée sur un support lui procurant stabilité et pérennité. Caractère exact et complet de l'information.

Actif informationnel non numérique
Information sur un support qui n'est pas numérique, par exemple, papier, microfilm, film, images imprimées, etc., se trouvant notamment dans un classeur, un tiroir, un porte-documents, un sac à dos, un bureau, un photocopieur, une imprimante, etc. Un actif informationnel non numérique qui a été numérisé est encore considéré comme un actif informationnel non numérique.

Renseignement personnel
Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu de la loi n'est pas considéré comme un renseignement personnel aux fins de la présente Politique.

Plan de rétablissement
Procédures visant à assurer l'application rapide et méthodique de mesures de rétablissement à la normale à la suite d'un incident. L'original du plan de rétablissement et ses éléments constitutifs doivent être conservés dans un lieu externe.

RSI – Responsable de la sécurité de l'information
Personne nommée par le conseil des commissaires chargée des communications avec les intervenants de la CSEM au sujet des orientations et des priorités liées à la sécurité de l'information.

Traçabilité
Situation où existe de l'information suffisante pour connaître (éventuellement de façon rétrospective) la composition d'un actif informationnel tout au long de sa chaîne de production, de transformation et de distribution, où que ce soit, depuis son origine jusqu'à la fin de son cycle de vie.