

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Responsabilité

Responsable de la sécurité de l'information (RSI)

Adoption

Adoptée par le Comité de gestion de la taxe scolaire de l'île de Montréal le 20 juin 2019 par la résolution 11.

Entrée en vigueur le

20 juin 2019



Comité de gestion
de la taxe scolaire
de l'île de Montréal

Comité de gestion de la taxe scolaire de l'île de Montréal

Table des matières

1. Préambule	3
2. Contexte	3
3. Objectifs	3
4. Cadre légal et administratif	4
5. Champ d'application	4
6. Principes directeurs	4
7. Catégorisation des actifs informationnels	5
8. Gestion des incidents	5
9. Écrits administratifs	6
10. Sensibilisation et formation	6
11. Sanctions	6
12. Diffusion et mise à jour de la Politique	6
13. Entrée en vigueur	6



1. Préambule

La Politique sur la sécurité de l'information (ci-après la « **Politique** ») définit le cadre général régissant l'utilisation des actifs informationnels du Comité de gestion de la taxe scolaire de l'île de Montréal (ci-après le « **CGTSIM** »). Elle permet au CGTSIM d'accomplir ses missions, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue (dont il est le gardien).

L'information liée aux ressources humaines, matérielles, technologiques et financières est accessible sur des formats numériques et non-numériques. Les risques d'atteinte à la disponibilité, intégrité ou confidentialité de ces informations peuvent avoir des conséquences liées à :

- La vie, la santé ou le bien-être des personnes;
- L'atteinte à la protection des renseignements personnels et à la vie privée;
- La prestation de services à la population;
- L'image du CGTSIM et du gouvernement.

2. Contexte

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGRI) (LRQ, Loi 133) et la Directive sur la sécurité de l'information gouvernementale (DSIG), une directive du Conseil du trésor du Québec, créent des obligations au CGTSIM en sa qualité d'organisme public.

Ainsi, la DSIG oblige le CGTSIM à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une Politique de sécurité de l'information en ayant recours notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Tel que requis par la loi, un Responsable de la sécurité de l'information (RSI) et un Coordonnateur sectoriel de la gestion des incidents (CSGI) sont désignés par le CGTSIM.

3. Objectifs

Par cette Politique, le CGTSIM affirme son engagement à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou ses moyens de communication. À cet égard, le CGTSIM doit veiller à :

- La **disponibilité** de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- L'**intégrité** de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- La **confidentialité** de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.



Le CGTSIM met en place cette Politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée par un cadre de gestion de la sécurité de l'information.

4. Cadre légal et administratif

La présente Politique s'inscrit, entre autres, dans le contexte législatif suivant :

- La Charte des droits et libertés de la personne (LRQ, chapitre C- 12);
- La *Loi sur l'instruction publique* (L.R.Q. c. I-13.3);
- La *Loi sur les archives* (L.R.Q. c. A-21.1)
- Le Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (L.R.Q. c. A-21.1, r.1);
- Le Code civil du Québec (LQ, 1991, chapitre 64);
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, Loi 133);
- La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A- 2.1);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2);
- La Directive sur la sécurité de l'information gouvernementale;
- Les Règlements, politiques, procédures et autres encadrements administratifs du CGTSIM;

5. Champ d'application

La présente Politique s'adresse aux utilisateurs de l'information du CGTSIM, c'est-à-dire, tout son personnel, quel que soit son statut, toute personne physique ou morale qui, à titre de partenaire, consultant, fournisseur ou visiteur, utilise ou a accès aux actifs informationnels du CGTSIM.

L'information visée est celle que le CGTSIM détient dans le cadre de ses activités, fonctions, pouvoirs et missions, quelle que soit sa nature ou le support utilisé, que sa conservation soit assurée par lui-même ou par un tiers.

6. Principes directeurs

Les principes directeurs qui guident les actions du CGTSIM en matière de sécurité de l'information sont les suivants :

- S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité;
- Reconnaître l'importance de la Politique de sécurité de l'information;
- Reconnaître que l'environnement technologique des actifs de l'information numérique et non-numérique est



- en changement constant et interconnecté avec le monde;
- Protéger l'information tout au long de son cycle de vie (création, traitement, destruction);
- S'assurer que chaque employé a accès au minimum d'information requis pour accomplir ses tâches normales;
- S'assurer que l'utilisation des ressources technologiques des actifs de l'information numérique et non-numérique par les utilisateurs doit être encadrée par une politique.

7. Catégorisation des actifs informationnels

Le CGTSIM doit procéder à une catégorisation des actifs informationnels qui permet de soutenir une analyse de risques et permet d'évaluer la valeur de l'information à protéger. Il peut, par la suite, justifier les mesures de sécurité à mettre en œuvre et à appliquer afin de fournir un niveau adéquat de sécurité.

Le niveau de protection de l'information est établi en fonction :

- De la nature de l'information et de son importance;
- Des probabilités d'accident, d'erreur ou de malveillance auxquelles elles sont exposées;
- Des conséquences de la matérialisation de ces risques;
- Du niveau de risque acceptable par le CGTSIM.

Une mise à jour annuelle de cette catégorisation devra être faite.

8. Gestion des incidents

Le CGTSIM déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires à l'obtention des buts suivants :

- Limiter l'occurrence des incidents en matière de sécurité de l'information;
- Gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés au MEES conformément à la DSGI.

Dans la gestion des incidents, le CGTSIM doit agir afin de prévenir toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.



9. Écrits administratifs

La direction générale s'assure de la mise en place de mesures concernant :

- La gestion des accès;
- La gestion des vulnérabilités et la protection du réseau;
- La gestion des copies de sauvegardes;
- Le plan de continuité des affaires;
- La protection des actifs et de l'information quel qu'en soit le format;
- La gestion des fournisseurs ayant accès à l'information détenue par le CGTSIM.

Les écrits administratifs doivent être transmis aux membres du personnel concerné.

10. Sensibilisation et formation

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, le personnel du CGTSIM doit être formé et sensibilisé à : la sécurité de l'information et des systèmes d'information du CGTSIM; aux directives de la sécurité; à la gestion des risques; à la gestion des incidents; aux menaces existantes; aux conséquences d'une atteinte à la sécurité et à leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes une fois par année ou au besoin.

11. Sanctions

Tout employé du CGTSIM qui contrevient à la présente Politique et aux directives qui en découlent s'expose à des interventions et/ou à des mesures disciplinaires, administratives ou légales.

12. Diffusion et mise à jour de la Politique

Le responsable de la sécurité informationnelle, assisté du comité de travail pour la sécurité de l'information, s'assure de la diffusion et de la mise à jour de la Politique sur la sécurité de l'information. Elle pourra être révisée lors de changements significatifs.

13. Entrée en vigueur

La présente Politique est entrée en vigueur à la date de son adoption, soit le 20 juin 2019.

