POLITIQUE DE SECURITE DE L'INFORMATION

Responsabilité
Service des technologies de l'information

Adoption
Séance du Conseil d'administration du 22 avril 2026
sommaire exécutif CA-32-202604-01

Entrée en vigueur le
1er juillet 2026

Centre de services scolaire de Montréal

Québec

Table des matières

Préambule et encadrement légal

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*[1] et la *Directive gouvernementale sur la sécurité de l'information*[2], une directive du Conseil du trésor du Québec applicable au Centre de services scolaire de Montréal (le « **CSSDM** »), créent des obligations pour les centres de services scolaires en leur qualité d'organismes publics. Cette directive gouvernementale oblige le CSSDM à adopter, mettre en œuvre, maintenir à jour et assurer l'application d'une politique sur la Sécurité de l'information. Ainsi, le CSSDM doit prévoir 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.

La présente *Politique de sécurité de l'information* (la « **Politique** ») permet au CSSDM d'accomplir ses missions, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'Information qu'il a créée ou reçue et dont il est le gardien. Cette Information liée aux ressources humaines, matérielles, technologiques et financières est accessible sur des formats numériques et non numériques. L'atteinte à sa disponibilité, son intégrité ou sa confidentialité peut 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 et l'image du CSSDM et du gouvernement.

La Politique s'inscrit principalement dans un contexte régi par :

- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. G-1.03) ;
- La *Directive gouvernementale sur la sécurité de l'information* ;
- La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* ;
- La *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C 1.1) ;
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1).

La présente *Politique de sécurité de l'information* ainsi que la *Politique relative à la gouvernance des données* du CSSDM assurent une gestion cohérente, sécuritaire et conforme des actifs informationnels et des données au sein de l'organisation.

Objectifs

1. La Politique a pour objectif d'affirmer l'engagement du CSSDM de s'acquitter pleinement de ses obligations à l'égard de la Sécurité de l'information, quels que soient les supports ou les moyens de communication, et d'orienter et déterminer la vision de l'organisation en la matière.

[1] ch. G-1.03.

[2] Décret 1514-2021, le 8 décembre 2021.

2. Plus précisément, le CSSDM doit veiller à :

   2.1. La Disponibilité de l'Information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées ;

   2.2. 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 ;

   2.3. 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.

3. Les modalités d'application de la Politique sont précisées dans le Cadre de gestion sur la sécurité de l'information (le « **Cadre de gestion** »).

4. Les comportements attendus des utilisateurs ainsi que les mécanismes de contrôle visant le respect de ces comportements attendus sont définis dans les Règles d'application de l'utilisation des technologies au Centre de services scolaire de Montréal (CSSDM) (les « **Règles d'application** »).

Champ d'application

5. La Politique vise la sécurité de tout Actif informationnel du CSSDM et s'adresse aux Utilisateurs des Actifs informationnels.

Définitions

6. Les termes définis et utilisés dans la Politique sont regroupés à l'**Annexe I – Définitions**. Ces définitions s'appliquent également au Cadre de gestion et aux Règles d'application.

Principes généraux

7. Les principes généraux qui guident les actions du CSSDM en matière de Sécurité de l'information sont les suivants :

   7.1. Le CSSDM adhère aux orientations et objectifs stratégiques gouvernementaux en matière de Sécurité de l'information et met en œuvre des pratiques reconnues, adaptées et généralement utilisées dans le domaine ;

   7.2. Le CSSDM reconnait que les Actifs informationnels détenus sont essentiels aux activités du CSSDM et assure leur protection adéquate tout au long de leur Cycle de vie, selon leur valeur, leur niveau de confidentialité et les risques auxquels ils sont exposés ;

   7.3. Le CSSDM identifie clairement l'Information à protéger, ses propriétaires et le niveau de sécurité requis, et préserve cette Information contre toute divulgation ou accès non autorisé

   ;

   7.4. L'environnement technologique des Actifs informationnels est en constante évolution et s'inscrit dans un écosystème mondial interconnecté ;

7.5. Chaque Utilisateur n'a accès qu'aux Informations nécessaires à l'exercice de ses fonctions ; à cet égard le CSSDM s'engage à sensibiliser et à former les Utilisateurs à la sécurité des Actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leurs obligations en la matière ;

7.6. Le CSSDM encadre l'utilisation des Actifs informationnels par des Règles d'application claires et appropriées.

Rôles et responsabilités

8. **Directeur général et Dirigeant d'organisme public**

8.1. Le Directeur général est le premier responsable de la Sécurité de l'information au CSSDM.

9. **Chef de la sécurité de l'information organisationnelle (CSIO)**

9.1. Le CSIO assume la responsabilité de la prise en charge globale de la Sécurité de l'information au sein du CSSDM.

10. **Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)**

10.1. Les COMSI (2) sont responsables de l'opérationnalisation de la Sécurité de l'information au CSSDM. Ils mettent en œuvre les processus de sécurité, coordonnent la gestion des incidents et des vulnérabilités, appuient le CSIO, assurent la veille et la communication des alertes, collaborent avec les unités internes et représentent le CSSDM au sein du réseau gouvernemental de cyberdéfense (Réseau d'alerte gouvernemental, CERT-Qc et MCN).

11. **Comité de Sécurité de l'information**

11.1. Le comité de Sécurité de l'information a pour mandat d'appuyer le CSIO dans la mise en place du Cadre de gestion ainsi que des différents éléments requis pour assurer la protection du CSSDM et la conformité aux exigences réglementaires. Comité à la fois tactique et opérationnel, il :

11.1.1 Développe et maintient le Cadre de gestion ;

11.1.2 Élabore les plans d'action et les bilans en Sécurité de l'information ;

11.1.3 Met en œuvre les activités de sensibilisation et de formation ;

11.1.4 Propose toute action nécessaire en matière de Sécurité de l'information.

11.2. Il constitue également un espace d'échange pour les parties prenantes ainsi qu'un lieu de suivi de l'évolution de la posture en Sécurité de l'information.

11.3. Il est composé des parties prenantes du CSSDM directement concernées ou impliquées dans la mise en œuvre de la Sécurité de l'information.

12. **Sous-comité de la gestion des Incidents**

12.1. Relevant du comité de Sécurité de l'information, le sous-comité de gestion des Incidents :

12.1.1 Constitue et maintient une équipe de réponse aux Incidents, incluant les incidents de sécurité numériques et non numériques, et établit la procédure officielle de gestion des Incidents.

12.1.2 Vérifie la présence et l'efficacité des contrôles de détection, afin d'assurer l'identification rapide des Incidents, qu'ils soient en cours ou déjà survenus.

12.1.3 Planifie et réalise des tests périodiques de réponse aux Incidents, afin d'évaluer et d'améliorer continuellement les mécanismes en place.

12.2. Le sous-comité est composé des COMSI, et selon la nature ou la gravité d'un Incident, peut être élargi au CSIO, à la direction générale, au secrétariat général, aux directeurs de services ou leurs représentants, ainsi qu'à tout employé jugé essentiel.

13. **Comité de continuité des services essentiels**

13.1. Le comité de continuité des services essentiels assure la planification, la coordination et le suivi des mesures permettant de maintenir ou de rétablir les services essentiels du CSSDM en cas d'interruption majeure ou de sinistre.

13.2. Il agit autant en contexte de préparation du plan de continuité des services essentiels (PCSE) qu'en situation de sinistre.

13.3. Les participants à ce comité sont le CSIO, les COMSI, la direction générale, le secrétariat général, les directions de services ainsi que tout employé jugé essentiel.

14. **Responsable de la continuité des services essentiels (RCS)**

14.1. Il s'agit de la personne responsable de la coordination du PCSE au CSSDM. À cet effet, cette personne a pour responsabilités, notamment :

14.1.1 De planifier et de coordonner les mises à l'essai et la maintenance du PCSE ;

14.1.2 D'assurer la formation et la sensibilisation du personnel concerné ;

14.1.3 De coordonner l'action du comité de continuité des services essentiels.

15. **Responsable sectoriel de la continuité des services essentiels (RSCS)**

15.1. Le responsable sectoriel de la continuité des services essentiels s'assure de maintenir à jour le volet du PCSE lié au processus qu'il supervise, ainsi que de la disponibilité des ressources nécessaires au maintien ou au rétablissement du processus en cas de sinistre.

15.2. Il assure également la supervision des responsables opérationnels des activités essentielles relevant de son processus.

15.3. Il collabore avec le RCS, le CSIO, les COMSI et le comité de continuité des services essentiels.

16. **Gestionnaires**

16.1. Informer et sensibiliser le personnel relevant de son autorité à la Politique, et s'assurer de leur compréhension et de leur adhésion.

16.2. Assurer le respect des mesures de sécurité dans l'usage des outils, équipements, accès, stockage et partage de l'Information, et intervenir en cas de pratiques non conformes.

16.3. Soutenir une culture de Sécurité de l'information en :

16.3.1 Donnant l'exemple en respectant la Politique ;

16.3.2 Encourageant et valorisant des comportements sécuritaires ;

16.3.3 Intégrant la Sécurité de l'information dans les pratiques quotidiennes de travail.

17. **Utilisateurs**

17.1. Les Utilisateurs doivent prendre connaissance de la présente Politique, des Règles d'application, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer en signant la déclaration jointe en annexe aux Règles d'application.

17.2. Les Utilisateurs doivent utiliser, dans le cadre des droits d'accès qui leur sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les Actifs informationnels mis à leur disposition en se limitant aux fins auxquelles ils sont destinés.

Toutefois, le matériel technologique fourni par le CSSDM, notamment les ordinateurs portables, tablettes et téléphones cellulaires, peut faire l'objet d'une utilisation personnelle accessoire, pour autant que celle-ci respecte les lois, les politiques, les règles d'application ainsi que les directives en vigueur, qu'elle n'entrave pas l'exercice des fonctions de l'Utilisateur et qu'elle ne compromette pas la Sécurité, la Disponibilité, l'Intégrité ou la Confidentialité des Actifs informationnels.

17.3. Les Utilisateurs doivent respecter les mesures de Sécurité de l'information mises en place sur leur poste de travail et sur tout équipement contenant des Informations à protéger et ne pas modifier leur configuration ou les désactiver.

17.4. Les Utilisateurs s'engagent à ne pas poser des actions sur le réseau du CSSDM de nature à compromettre son Intégrité et sa sécurité, ne pas essayer d'en découvrir ou d'en exploiter les lacunes.

17.5. Les Utilisateurs doivent se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister et agir en conformité avec les droits que leur confère toute Licence logicielle s'appliquant à leurs outils technologiques.

17.6. Les Utilisateurs signalent immédiatement à leur supérieur tout acte dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des règles de Sécurité de l'information ainsi que toute anomalie pouvant nuire à la protection des Actifs informationnels du CSSDM.

Sanction

18. Tout manquement à la présente Politique peut entraîner des sanctions administratives ou disciplinaires selon la nature, la gravité et les conséquences de la contravention.

Entrée en vigueur

19. Cette Politique entre en vigueur au moment de son adoption par le Conseil d'administration ou à tout moment ultérieur qu'il détermine.

Annexe I – Définitions

1. **Actif informationnel :**

Tout actif, numérique ou non numérique, sur lequel reposent des données : Information, base de données, Document papier, système ou support d'Information, technologie de l'Information, installation ou ensemble de ces éléments acquis ou constitués par le CSSDM.

Cela inclut l'information et les supports permettant son traitement, sa transmission ou sa conservation, qu'ils soient électroniques (ordinateurs, tablettes, téléphones intelligents, Logiciels, serveurs, messagerie) ou traditionnels (papier, classeur, microfilm).

2. **Actif informationnel numérique :**

Toute Information stockée sous format numérique sur un support tel que disque, base de données, clé USB, mémoire flash, ordinateur, tablette, téléphone intelligent, vidéo ou photo numérique, etc.

L'Information sur ces supports peut être écrite, modifiée, copiée, cryptée ou effacée.

3. **Actif informationnel non numérique :**

Toute Information conservée sur un support physique tel que papier, microfilm, pellicule ou photo papier.

Une fois produite, l'Information sur le support de l'Actif non numérique ne peut être modifiée, copiée, cryptée ou effacée.

Les Actifs informationnels non numériques sont facilement déplaçables et peuvent exister en plusieurs exemplaires et à différents endroits, ce qui rend leur traçabilité difficile.

Lorsqu'un Actif non numérique est numérisé, il devient un Actif numérique. L'Information peut varier d'une copie à l'autre (ex. : un plan d'intervention signé à différents moments).

4. **Confidentialité, Confidentiel :**

Caractère d'un renseignement ou d'un Document dont la communication peut avoir des conséquences sur la vie privée des personnes ou sur les intérêts économiques et juridiques du CSSDM. Sauf exception, ces renseignements ne doivent pas être divulgués à une personne qui ne dispose pas des autorisations requises. Les Renseignements personnels sont de nature Confidentielle.

5. **Cycle de vie :**

Ensemble des étapes que franchit un Actif informationnel, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation du CSSDM.

6. **Disponibilité :**

Propriété d'une Information d'être accessible en temps voulu et de la manière requise par une personne disposant des accès et des autorisations requises.

7. **Document :**

Un Document est constitué d'Information portée par un support. L'Information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'Information peut être rendue au moyen de tout mode d'écriture y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles. Est assimilé au Document, toute banque de données dont les éléments structurants permettent la création de Documents par la délimitation et la structuration de l'Information qui y est inscrite (**article 3 de la Loi concernant le cadre juridique des technologies de l'Information).**

8. **Incident :**

Événement qui porte atteinte ou qui est susceptible de porter atteinte à la Disponibilité, à l'Intégrité ou à la Confidentialité de l'Information, ou plus généralement à la Sécurité de l'information, par exemple en causant une interruption des services ou une réduction de leur qualité.

9. **Information :**

Renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

10. **Intégrité :**

Renvoie au caractère complet et non altéré de l'état d'un Document. L'Intégrité est assurée lorsqu'il est possible de vérifier que l'Information n'est pas altérée, qu'elle est maintenue dans son intégralité et que le support qui porte cette Information lui procure la stabilité et la pérennité voulue. Pour assurer l'Intégrité, les modifications doivent être documentées et accompagner l'Information (Documents et Documents technologiques) tout au long de son Cycle de vie.

11. **Licence logicielle :**

Contrat par lequel le propriétaire des droits du Logiciel autorise un Utilisateur à poser les gestes suivants selon des termes prescrits : installer le Logiciel, l'utiliser, faire une copie de sauvegarde. La Licence logicielle définit les droits d'utilisation pour un Logiciel propriétaire ou libre.

12. **Logiciel :**

Ensemble d'Informations relatives à des traitements effectués automatiquement par un Outil technologique et stockées sous forme d'un ensemble de fichiers dans une mémoire, un disque dur ou un média prévu à cette fin ; un Logiciel est généralement destiné à assister un Utilisateur dans une de ses activités, d'où le synonyme d'application souvent utilisé pour désigner un Logiciel requis pour l'exécution d'une tâche donnée (traitement de texte, production de la paie, jeux, outils d'intelligence artificielle, etc.).

Un Logiciel libre est un Logiciel dont l'utilisation, l'étude, la modification et la duplication en vue de sa diffusion sont permises, techniquement et légalement, sans frais.

Un Logiciel propriétaire est un Logiciel dont l'utilisation, l'étude, la modification et la duplication en vue de sa diffusion sont régies par une Licence logicielle qui doit être acquise et généralement achetée.

Le terme Logiciel inclut notamment :

- Logiciel installé sur un poste de travail ou un appareil mobile ;
- Application disponible via une plateforme Web ;
- Extension ou complément intégré à un navigateur Web ;
- Outil intégré à la suite Microsoft 365, incluant Teams, SharePoint et les applications Office (version de bureau et en ligne).

13. **Outil technologique :**

Tout dispositif exploité par un Utilisateur comportant des composantes électroniques et lui permettant d'accomplir une activité donnée, notamment les suivants :

- Ordinateur de table ou portable
- Tablette numérique
- Téléphone cellulaire
- Téléphone IP
- Tableau numérique interactif/Écran interactif et autres périphériques d'entrée de données
- Imprimante et autres outils permettant la reproduction de données
- Tout autre outil permettant un lien à Internet

14. **Renseignement personnel :**

Renseignement sur l'identité d'une personne physique permettant de l'identifier directement ou indirectement.

15. **Sécurité de l'information :**

Protection de l'Information contre les risques et les Incidents. Le terme sécurité fait autant référence à la cybersécurité qu'à la Sécurité de l'information.

16. **Utilisateur :**

Toute personne, employé, parent ou toute autre personne physique qui accède par le truchement des réseaux numériques et non numériques à de l'Information que le CSSDM détient dans l'accomplissement de sa mission. Les membres du personnel du CSSDM ainsi que les élèves sont les premiers Utilisateurs de l'Information du CSSDM. Tout Utilisateur de ces réseaux doit se conformer aux politiques et aux directives en vigueur au CSSDM dans le cadre de toutes ses activités lorsqu'il y partage des Actifs informationnels ou des dispositifs de technologies de l'Information.

Quiconque utilise un Outil technologique fourni par le CSSDM ou une composante de l'infrastructure informatique du CSSDM et ayant un lien fonctionnel avec le CSSDM, notamment les personnes suivantes :

- Membres du personnel
- Élèves jeunes et adultes
- Parents
- Membres du Conseil d'administration
- Bénévoles
- Stagiaires
- Consultants
- Employés contractuels
- Sous-traitants
- Organismes externes

Pour joindre le service responsable :
ti@cssdm.gouv.qc.ca

cssdm.gouv.qc.ca

Centre
de services scolaire
de Montréal
Québec