Commission scolaire de Montréal

D2019-4

Directive sur la sécurité de l'information

Présentée au CC	**Modification**
19 juin 2019 **Entrée en vigueur** 20 juin 2019	

Table des matières

Commission scolaire de Montréal

Directive sur la sécurité de l'information

Direction générale de la Commission scolaire de Montréal

Cette page est laissée vide intentionnellement

Commission scolaire de Montréal

HISTORIQUE

Auteur	Rôle	Description	Date
André Bachand	Conseiller principal de la SI – Projet SICS	• Création	2017-11-28
André Bachand	Conseiller principal de la SI – Projet SICS	• Approbation par le MEES	2018-02-14
André Bachand	Conseiller principal de la SI – Projet SICS	• Transfert des sections 6, 7, 8, 9, 10 vers le cadre de gestion	2018-05-04
Lucie Perreault et Comité de sécurité	Directrice du STI Resp. Sécurité de l'information	• Adaptation pour la CSDM	2019-12-12 au 2019-02-05
Guy Nicol	Analyste au STI	• Intégration des sections sécurité et droits d'auteurs en provenance de la Politique d'utilisation	2013-03-13 au 2019-03-25
Guy Nicol	Analyste au STI	• Uniformisation	2019-03-26 au 2019-05-02
Guy Nicol Comité de sécurité Sylvie Gallant	Analyste au STI Membres du comité de sécurité Secrétaire générale	• Révision finale	2019-05-03 au 2019-06-13

Commission scolaire de Montréal

TABLE DES MATIERES

1. CONTEXTE

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) (LRQ, Loi 133) et de la Directive sur la sécurité de l'information gouvernementale (DSIG) (une directive du Conseil du trésor du Québec applicable à la CSDM) créent des obligations aux établissements scolaires en leur qualité d'organismes publics.

Ainsi, la Directive sur la sécurité de l'information gouvernementale oblige la CSDM à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une directive de sécurité de l'information – dont les principales modalités sont définies dans la directive gouvernementale – 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. Ceci demande que 2 rôles soient comblés au sein de chaque commission scolaire. Tel qu'il est stipulé dans le ***Guide de nomination***, un Responsable de la sécurité de l'information (RSI) et deux (2) Coordonnateurs sectoriels de la gestion des incidents (CSGI) doivent être désignés.

Cette directive permet à la CSDM 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 elle est la gardienne). Cette information liée aux ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et non numériques, dont les risques d'atteinte à sa disponibilité, intégrité ou confidentialité 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 de la CSDM et du gouvernement

2. OBJECTIFS

La présente directive a pour objectif d'affirmer l'engagement de la CSDM à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication.
Plus précisément, la CSDM 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.

Par conséquent, la CSDM met en place cette directive dans le but d'orienter et de déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information et de l'utilisation des technologies de la CSDM.

Veuillez vous référer au document « **Cadre de gestion de la Directive sur la sécurité de l'information et de l'utilisation des technologies à la Commission scolaire de Montréal** » pour plus de détails.

3. CADRE LÉGAL ET ADMINISTRATIF

La Directive de sécurité s'inscrit principalement dans un contexte régi par :

- La Charte des droits et libertés de la personne (LRQ, chapitre C-12)
- La loi sur l'instruction publique (L.R.Q. c. l-13.3)
- 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 Code criminel (LRC, 1985, chapitre C-46)
- 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
- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42)
- Politique concernant le Code de déontologie et d'éthique relatif à l'utilisation des technologies à la Commission scolaire de Montréal (2014-06-21)
- Modalité d'application de la Politique concernant le Code de déontologie et d'éthique relatif à l'utilisation des technologies à la Commission scolaire de Montréal (2014-06-21)
- L'éthique et les valeurs au travail: code de conduite des employés de la CSDM (2017-02-22) et modifications (2017-11-22)

4. CHAMP D'APPLICATION

La présente directive s'adresse aux utilisateurs de l'information, c'est-à-dire à tout le personnel, à toute personne physique ou morale qui à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public utilise les actifs informationnels de la CSDM. Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par la CSDM.
À cette fin, il doit :

4.1 Prendre connaissance de la présente directive, 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 du cadre de gestion.

4.2 Utiliser, 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 mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés.

4.3 Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver.

4.4 S'engager à ne pas poser des actions sur le réseau de la CSDM de nature à compromettre son intégrité et sa sécurité. Ne pas essayer d'en découvrir ou d'en exploiter les lacunes.

4.5 S'engager à ne pas utiliser d'outils qui permettent d'accéder de façon illégale aux données non requises pour son travail ou ses apprentissages, risquant de nuire à sa sécurité.

4.6 S'engager à ne pas faire des recherches non autorisées sur le réseau.

4.7 S'assurer que l'outil technologique personnel utilisé sur le réseau de la CSDM est prémuni contre les logiciels malveillants. Ne pas accéder au réseau de la CSDM par l'entremise d'un ordinateur ne disposant pas d'une protection logicielle à cet effet (antivirus) qui soit à jour, et ce, peu importe le système d'exploitation utilisé par l'ordinateur.

4.8 Ne pas poser d'acte visant à détruire ou à porter atteinte à l'intégrité des données des autres utilisateurs ou des données en provenance d'autres organismes.

4.9 Respecter les règles associées à la réception et à la divulgation des renseignements personnels et confidentiels en vigueur à la CSDM.

4.10 S'engager à ne pas modifier ou détruire un logiciel ou une banque de données sans l'autorisation du gestionnaire de l'unité qui en assure le développement et le soutien.

4.11 S'engager à utiliser les outils technologiques selon les droits qui lui sont accordés, sans jamais tenter de forcer les mesures de sécurité mises en place afin de protéger les systèmes informatiques de la CSDM.

4.12 Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister.

4.13 Agir en conformité avec les droits que lui confère toute licence logicielle s'appliquant à ses outils technologiques.

4.14 S'abstenir de faire usage de reproductions illicites d'un logiciel propriétaire ou de participer de manière directe ou indirecte à une telle reproduction.

4.15 S'engager à respecter les droits de propriété intellectuelle des données ou des contenus qu'il utilise.

4.16 Porter une attention particulière aux droits associés aux contenus publiés sur Internet : s'assurer qu'il dispose des autorisations requises avant d'intégrer à ses documents et autres productions réalisées numériquement des images, des textes, du code de programmation ou toute autre donnée récupérée sur Internet.

4.17 Signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la CSDM.

L'information visée est celle que la CSDM détient dans le cadre de ses activités, que sa conservation soit assurée par elle-même ou par un tiers. Les formats de l'information visée sont numériques et non numériques.

Veuillez vous référer au document « **Glossaire de la sécurité de l'information et de l'utilisation des technologies** » pour une liste détaillée des rôles et responsabilités.

5. PRINCIPES DIRECTEURS

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

5.1 S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité.

5.2 Reconnaître l'importance de la directive de sécurité de l'information.

5.3 Reconnaître que l'environnement technologique des actifs informationnels numériques et non numériques est en changement constant et interconnecté avec le monde.

5.4 Protéger l'information tout au long de son cycle de vie (création, traitement, destruction).

5.5 S'assurer que chaque employé n'ait accès qu'au minimum d'information requis pour accomplir ses tâches normales.

5.6 Encadrer l'utilisation par les utilisateurs des actifs informationnels numériques et non numériques par des lignes directrices qui expliquent une marche à suivre appropriée, qui indique ce qui est permis et ce qui ne l'est pas.

Veuillez vous référer au document « ***Lignes directrices sur l'utilisation des technologies à la Commission scolaire de Montréal*** » pour plus de détails.

6. SANCTION

Tout employé de la CSDM qui contrevient au cadre légal, à la présente directive et aux mesures de sécurité de l'information qui en découlent, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles disciplinaires internes applicables (dont celles des conventions collectives de travail et des Règlements de la CSDM).

Les fournisseurs, partenaires, invités, consultants ou organismes externes sont aussi passibles de ces sanctions.

7. DIFFUSION ET MISE À JOUR DE LA DIRECTIVE

Le RSI, assisté du comité de travail pour la sécurité de l'information, s'assure de la diffusion et de la mise à jour de la directive. La directive de sécurité de l'information sera révisée périodiquement selon les mises à jour effectuées.

8. ENTRÉE EN VIGUEUR

La présente directive entre en vigueur à la date de son adoption par le conseil des commissaires.

Commission scolaire de Montréal

Cadre de gestion de la sécurité de l'information et de l'utilisation des technologies

Direction générale de la Commission scolaire de Montréal

Cette page est laissée vide intentionnellement

Commission scolaire de Montréal

HISTORIQUE

Auteur	Rôle	Description	Date
André Bachand	Conseiller principal de la SI – Projet SICS	• Création	2017-11-28
André Bachand	Conseiller principal de la SI – Projet SICS	• Approbation	2018-02-14
André Bachand	Conseiller principal de la SI – Projet SICS	• Documenter les comités de gestion d'incidents et continuité des affaires	2018-03-20
André Bachand	Conseiller principal de la SI – Projet SICS	• Ajouter sections 6, 7, 8, 9, 10 venant de la politique SI	2018-05-04
Lucie Perreault et Comité de sécurité	Directrice du STI Resp. Sécurité de l'information	• Adaptation pour la CSDM	2019-12-12 au 2019-02-05
Guy Nicol	Analyste au STI	• Adaptation pour la CSDM • Intégration de la directive sur l'utilisation des technologies	2019-03-13 au 2019-03-21
Guy Nicol	Analyste au STI	• Uniformisation • Intégration d'informations en provenance du Guide de nomination	2019-03-26 au 2019-05-02
Guy Nicol Comité de sécurité Sylvie Gallant	Analyste au STI Membres du comité de sécurité Sécrétaire générale	• Révision finale	2019-05-03 au 2019-06-13

Commission scolaire de Montréal

TABLE DES MATIERES

Commission scolaire de Montréal

PRÉAMBULE

Le cadre de gestion de la sécurité de l'information et de l'utilisation des technologies renforce les systèmes de contrôle internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins de la CSDM en matière de réduction du risque associés à la protection de l'information.

Ce cadre de gestion s'applique à la :

- **Directive sur la sécurité de l'information**, ci-après nommée **Directive de sécurité**

ainsi qu'aux :

- **Lignes directrices sur l'utilisation des technologies**, ci-après nommée **Lignes directrices d'utilisation**

La sécurité de l'information

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) (LRQ, Loi 133) et de la Directive sur la sécurité de l'information gouvernementale (DSIG) (une directive du Conseil du trésor du Québec applicable à la CSDM) créent des obligations aux commissions scolaires en leur qualité d'organismes publics.

Ainsi, la Directive sur la sécurité de l'information gouvernementale oblige la CSDM à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de sécurité de l'information – dont les principales modalités sont définies dans la directive gouvernementale – 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. Pour ce faire, la CSDM se dote du présent cadre de gestion qui permettra aux différents niveaux de gestion de travailler ensemble pour optimiser la mise en place des initiatives de sécurité liées à la politique de la sécurité de l'information.

L'utilisation des technologies

Depuis plusieurs années, la CSDM possède un code de déontologie et d'éthique relatif à l'utilisation des technologies. Sous sa forme précédente, ce code servait à indiquer les comportements attendus, à définir les principes directeurs et à mettre en place quelques mesures de sécurité.

Avec l'arrivée de la **Directive sur la sécurité de l'information**, le code de déontologie et d'éthique relatif à l'utilisation des technologies devient les **Lignes directrices sur l'utilisation des technologies**, ci-après nommée **Lignes directrices d'utilisation**. Dans ces **Lignes directrices d'utilisation**, les éléments relatifs à la sécurité de l'information ont été retirés et sont entièrement traités dans la **Directive de sécurité**.

Le cadre de gestion constitue un document administratif balisant l'application des **Lignes directrices d'utilisation** en énonçant les droits, responsabilités et obligations des différents paliers d'autorité à la CSDM. Il comporte également des modalités précises qui concernent

l'attribution de droits particuliers d'accès au réseau et précise les attentes de la CSDM concernant le comportement de son personnel de soutien informatique.

OBJECTIFS

Le présent cadre de gestion a pour objectif d'identifier les divers intervenants et les différents comités en définissant leurs responsabilités pour permettre à la CSDM de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information et de l'utilisation des technologies.

Plus précisément :

- Le Conseil des commissaires
- La direction générale et son comité de direction
- Le comité de la sécurité de l'information
- Le sous-comité de la gestion d'incidents
- Le sous-comité de la continuité des affaires
- L'ensemble des gestionnaires
- Le Service de la gestion des personnes et du développement des compétences (SGPDC)
- Le Service des technologies de l'information

Par conséquent, la CSDM met en place ce cadre dans le but d'instaurer la synergie entre les différents intervenants qui permettra une mise en œuvre des obligations découlant de la **Directive de sécurité** et des **Lignes directrices d'utilisation**.

1. CADRE LÉGAL ET ADMINISTRATIF

Le cadre de gestion s'inscrit dans un contexte régi par le cadre légal et administratif défini au sein de la **Directive de sécurité** et des **Lignes directrices d'utilisation** adoptées par la CSDM.

2. CHAMP D'APPLICATION

Le présent cadre s'adresse aux divers groupes mentionnés ci-dessus incluant les membres des trois comités, c'est-à-dire à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'élève ou de public, siège à un des comités suivants : Comité de la sécurité de l'information, Sous-comité de la gestion d'incidents et Sous-comité de la continuité des affaires.

3. GESTION DES RISQUES

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

La gestion des risques liés à la sécurité de l'information numérique et non numérique s'inscrit dans le processus global de gestion des risques de la CSDM. Les risques à portée gouvernementale sont déclarés conformément à la Directive de la sécurité de l'information gouvernementale. L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information et l'utilisation des technologies, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement à la CSDM.

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 la CSDM.

4. GESTION DES INCIDENTS

La CSDM déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, elle 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 Directive sur la sécurité de l'information gouvernementale.

Dans la gestion des incidents, la CSDM peut exercer ses pouvoirs et ses prérogatives à l'égard de toute utilisation inappropriée de l'information qu'elle détient ou de ses systèmes d'information.

5. MODALITÉS

Pour chacune des modalités élaborées ci-dessous, prévoir une révision à fréquence prédéterminée et procéder à une mise à jour au besoin.

Gestion des accès

Une gestion des accès logiques et physiques doit être élaborée, encadrée et contrôlée pour faire en sorte de protéger la disponibilité, l'intégrité et la confidentialité de l'information numérique et non numérique. Cette gestion doit inclure l'approbation, la revalidation et la destruction de ces accès et la conservation des preuves pour les audits ultérieurs.

Gestion des vulnérabilités

La CSDM déploie des mesures pour maintenir à jour son parc informatique afin de maintenir les vulnérabilités des actifs informationnels numérique et non numérique à son niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une mesure de notification des vulnérabilités venant des fournisseurs doit être mise en place pour les corriger.

Gestion des copies de sauvegardes

La CSDM doit élaborer une stratégie de copie de sauvegarde pour se prémunir contre une perte de données numériques et non numériques. Cette stratégie doit inclure la rétention des copies, les alertes d'erreurs lors de la prise de copie et les tests de restauration de ces copies à une fréquence adéquate.

Continuité des affaires

La CSDM doit élaborer une stratégie de continuité des affaires advenant qu'un incident cause l'arrêt de la prestation de service. Cette stratégie doit être testée à une fréquence adéquate et les écarts doivent être corrigés.

Protection du périmètre du réseau

La CSDM doit instaurer des exercices de tests d'intrusion et de balayages de vulnérabilités pour identifier les points d'entrée susceptibles de donner un accès inapproprié à des individus ou des programmes malicieux. De plus, un système de prévention et de détection d'intrusions devrait être mis en place pour augmenter le niveau de protection

Utilisation d'un appareil personnel (B.Y.O.D)

Une ligne directrice sur l'utilisation d'un appareil personnel (iPad, téléphone intelligent, etc.) dans l'exercice de ses fonctions doit être élaborée pour bien encadrer cette pratique. Les données de la CSDM doivent être protégées.

Protection des actifs informationnels en format non numérique

La CSDM doit se doter d'une ligne directrice de protection des actifs informationnels non numériques. Une notion de bureau propre doit être instaurée. Ces actifs non numériques peuvent être transportés et produits en plusieurs exemplaires. La notion d'archivage et de destruction doivent être considérée dans l'élaboration de cette ligne directrice. Cette protection inclut la gestion des accès physiques aux salles, aux imprimantes ou aux autres endroits qui détiennent des actifs informationnels non numériques. Cette ligne directrice de la protection du périmètre prévoit faire des tests d'intrusions ainsi de les protéger lors du transit d'un endroit à un autre.

Gestion des fournisseurs

La CSDM doit mettre en place un processus de gestion de ses fournisseurs pour s'assurer qu'ils ne viendront pas causer des incidents, des divulgations/pertes de données ou introduire des virus sur son réseau. Pour ce faire, le fournisseur doit signer une entente stipulant qu'il s'engage à répondre aux exigences en cybersécurité de la CSDM et que la CSDM est en droit de voir les résultats des audits (3416, SOC2, etc.) conduits sur ce fournisseur. Cette entente doit aussi inclure les objectifs/niveaux de service attendus par ce fournisseur. Les fournisseurs ont accès à l'information sensible de la CSDM et doivent signer une entente de confidentialité dans le but de diminuer le risque d'une divulgation de cette information.

L'Internet des objets (IDO) en anglais IOT

La CSDM doit mettre en place un encadrement pour l'Internet des objets. L'IDO décuple la force de frappe d'une cyberattaque du type **Déni de service distribué** (DDOS), augmente la surface d'attaque et les données personnelles peuvent se retrouver à un plus grand nombre d'endroits.

6. CADRE DE GESTION

Le cadre de gestion de la sécurité de l'information et de l'utilisation des technologies renforce les systèmes de contrôle internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins de la CSDM en matière de réduction du risque associés à la protection de l'information.

Conseil des commissaires

Le Conseil des commissaires approuve la nomination des responsables en sécurité de l'information désignés pour la CSDM et adopte la **Directive sur la sécurité de l'information** ainsi que toute modification à celle-ci. Par ailleurs, le Conseil est régulièrement informé des actions de la CSDM en matière de sécurité de l'information.

Direction générale et son comité de direction

La Direction générale de la CSDM, étant le premier responsable de la sécurité de l'information au sein de sa commission scolaire, détermine des mesures visant à favoriser l'application de la politique et des obligations légales de la CSDM en matière de sécurité de l'information. Ainsi, avec les membres de son comité de direction (CCDG), elle détermine les orientations stratégiques, les plans d'action et les bilans de sécurité de l'information. Elle peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application des Directives de sécurité et d'utilisation.

La Direction générale approuve aussi les normes et modalités d'application de la Directive sur l'utilisation des technologies de même que toute modification au document initial.

Comité de la sécurité de l'information

Le comité de la sécurité de l'information a comme objectif d'assister le responsable de la sécurité de l'information (RSI) à mettre en place le cadre de gestion de la sécurité de l'information et des autres éléments pouvant être nécessaires pour assurer la protection de la CSDM et être conforme à la réglementation. C'est un comité qui est tactique et opérationnel.

Ce comité est chargé de réaliser le cadre de gestion, les plans d'action et les bilans de sécurité de l'information, les activités de sensibilisation ou de formation ainsi que toute proposition d'action en matière de sécurité de l'information. C'est aussi un forum d'échange entre les parties prenantes ou d'observation de l'évolution du projet en sécurité de l'information.

Le comité est formé des parties prenantes de la CSDM qui seront directement concernées ou qui participent à la mise en œuvre de la sécurité de l'information.

Sous-comité de la gestion des incidents

Ce sous-comité relève du comité de la sécurité de l'information. Le sous-comité de la gestion des incidents a la responsabilité de monter et maintenir opérationnelle une équipe de réponse aux incidents de sécurité numériques et non numériques et d'établir une procédure de réponses aux incidents. Ce sous-comité doit comprendre les CSGI et au besoin le RSI, la Direction générale, le Secrétariat général, les directeurs de services ou leurs représentants délégués selon

la criticité de l'évènement ainsi que tous employés jugés essentiels. Le sous-comité doit s'assurer que les contrôles sont en place pour identifier un incident lorsqu'il se produit ou s'est produit. Le sous-comité doit s'assurer que des tests de réponse aux incidents soient conduits périodiquement pour vérifier l'efficacité des contrôles en place.

Sous-comité de la continuité des affaires

Le sous-comité de la continuité des affaires doit faire l'analyse des processus d'affaires de la CSDM et identifier ceux qui auront un impact majeur à la CSDM s'ils venaient à ne plus être fonctionnels et que la prestation de services était arrêtée. Ce sous-comité doit prévoir réaliser des tests de continuités des affaires pour en valider l'efficacité. Les participants de ce sous-comité sont le RSI, les CSGI, la Direction générale, le Secrétariat général, les directeurs de services ainsi que tous employés jugés essentiels.

7. RÔLES ET RESPONSABILITÉS

Direction générale

La Direction générale doit :

- Désigner les principaux intervenants en sécurité de l'information.
- Mettre en œuvre une directive et un cadre de gestion de la sécurité de l'information.
- Définir et mettre en place les processus majeurs de sécurité de l'information.
- Présenter régulièrement au Ministère un plan d'action et un bilan de sécurité de l'information.
- Déclarer aux instances concernées les incidents de sécurité de l'information à portée gouvernementale ainsi que les risques de sécurité de l'information à portée gouvernementale.
- S'assurer que l'ensemble des dispositions de la **Directive de sécurité** et des **Lignes directrices d'utilisation** soient observés par les services et les établissements sous sa gouverne.
- Voir à l'autorisation des demandes de dérogation visant la restriction des accès à Internet pour un groupe d'utilisateurs au sein d'une unité administrative, d'une école ou d'un centre.

Conseil des commissaires

- Adopter la **Directive de sécurité**.

Responsable de la sécurité de l'information (RSI)

Le responsable de la sécurité de l'information doit :

- Conseiller la haute direction au sujet des orientations et des priorités en matière de sécurité de l'information.
- Assurer l'arrimage de toutes les préoccupations en matière de sécurité de l'information.
- Communiquer à la CSDM les orientations et les priorités d'intervention gouvernementales.
- S'assurer de la participation de la CSDM à la mise en œuvre des processus officiels de la gestion de la sécurité de l'information.
- Assurer la coordination et la cohérence des actions de la sécurité de l'information menées par d'autres acteurs : détenteurs de l'information et autres responsables (ressources

informationnelles, accès à l'information et protection des renseignements personnels, gestion documentaire, sécurité physique et éthique).

- Établir des liens avec les RSI des autres commissions scolaires afin de partager les expertises et les stratégies à développer et à mettre en œuvre.
- Coordonner l'élaboration des processus officiels de la sécurité de l'information à la CSDM.
- Mettre en place et animer les comités internes de coordination et de concertation en sécurité de l'information au sein de la CSDM.
- Coordonner l'élaboration d'un programme officiel et continu de formation et de sensibilisation en matière de sécurité de l'information pour tout le personnel de la CSDM.
- Instaurer un processus de veille sur les menaces, les vulnérabilités et les bonnes pratiques de sécurité de l'information.
- Soumettre à la direction générale les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes incluant le bilan des réalisations ainsi que tout évènement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information de la CSDM.

Coordonnateur sectoriel de la gestion des incidents (CSGI)

Le Coordonnateur sectoriel de la gestion des incidents doit :

- Contribuer à la mise en œuvre des processus officiels de la sécurité de l'information de la CSDM
- Établir des liens avec les CSGI des autres commissions scolaires afin de partager les expertises et les stratégies à développer et à mettre en œuvre.
- Coordonner la gestion des incidents à portée gouvernementale :
  - Mettre en place une équipe de réponse aux incidents pour la CSDM.
  - Développer, mettre en place et tester un plan de réponse aux incidents de sécurité pour la CSDM.
  - Participer au processus gouvernemental de gestion des incidents et au réseau d'alerte gouvernemental.
- Contribuer aux analyses des risques de la sécurité de l'information, définir les menaces et les situations de vulnérabilité et mettre en œuvre les solutions appropriées pour la CSDM.
- Contribuer à l'autoévaluation de la sécurité des systèmes et des réseaux informatiques de la CSDM par des exercices d'audit de sécurité et des tests d'intrusion pour les systèmes jugés à risques.
- Tenir à jour les guides sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications mis en place à la CSDM.
- Maintenir une veille continue sur les risques, les menaces et les vulnérabilités.

Secrétariat général

Le secrétariat général s'assure de l'adoption de la **Directive de sécurité** par le Conseil des commissaires et de la publication de cette information sur le site Web de la CSDM.

Ensemble des gestionnaires

Les droits et responsabilités des gestionnaires concernent la mise en œuvre de la **Directive de sécurité**, des **Lignes directrices d'utilisation**, de même que l'encadrement des utilisateurs.

- Tout gestionnaire de la CSDM est responsable de faire en sorte que, pour tous les utilisateurs sous sa responsabilité, la **Directive de sécurité** et les **Lignes directrices d'utilisation** soient connues et bien comprises. De cette responsabilité découle une obligation d'éducation, de même qu'une obligation de supervision.
- Tout gestionnaire au sein d'un établissement d'enseignement doit s'assurer qu'une surveillance adéquate est exercée par l'ensemble du personnel sous sa responsabilité à l'endroit des élèves qui utilisent un outil technologique, afin d'éviter que ces derniers démontrent des comportements répréhensibles ou encore accèdent à des sites, des logiciels ou des forums de discussion qui contreviennent à la Directive de sécurité ou aux **Lignes directrices d'utilisation**.
- Tout gestionnaire doit intervenir lorsqu'il constate ou suspecte qu'un utilisateur déroge à l'esprit ou à la lettre de la Directive de sécurité ou des **Lignes directrices d'utilisation**.
- Les interventions du gestionnaire devront respecter les principes liés à l'intervention disciplinaire sur le plan de la gradation et de l'intensité.
- Le Service de la gestion des personnes et du développement des compétences peut émettre des recommandations, à la demande du gestionnaire concerné, quant à la nature des sanctions à imposer à un utilisateur en fonction des critères habituels, notamment le caractère chronique du comportement justifiant une sanction de même que son impact sur le bon fonctionnement de la CSDM.
- Tout gestionnaire peut demander une vérification du comportement d'un utilisateur, sans son consentement et sans avis, s'il a des motifs raisonnables de croire qu'une telle vérification est nécessaire. Cette demande de vérification doit se faire auprès du bureau des relations professionnelles et peut concerner l'un des aspects suivants :
  - Historique de navigation sur Internet.
  - Contenu d'un ordinateur ou d'un autre outil technologique.
  - Contenu d'un serveur de fichiers.
  - Utilisation et contenu du courriel.
  - Utilisation de la téléphonie IP et contenu de la boite vocale.
  - Toute autre trace d'utilisation d'un outil technologique pouvant témoigner d'une inconduite de l'utilisateur.
- Le gestionnaire peut demander qu'une surveillance active du comportement d'un utilisateur soit faite, s'il a des motifs raisonnables de croire qu'une telle surveillance est requise. Selon la nature du comportement suspecté et justifiant la demande de surveillance, le gestionnaire déterminera si un avis doit être transmis à l'utilisateur préalablement à cette surveillance. Tous les frais liés aux dispositifs technologiques et aux travaux nécessaires afin d'opérer cette surveillance active seront cependant à la charge de l'unité requérante, sauf dans le cas d'activités criminelles suspectées ou d'atteinte à la sécurité de l'information.

- Le gestionnaire peut demander que des restrictions d'accès aux outils technologiques ou aux infrastructures soient appliquées pour un utilisateur, sous réserve de la faisabilité technique de ces restrictions.
- Le gestionnaire peut demander, pour un groupe d'utilisateurs ou pour l'ensemble des utilisateurs sous sa gouverne, que des restrictions particulières d'accès aux outils technologiques ou aux infrastructures soient appliquées, sous réserve de l'approbation d'un gestionnaire titulaire de budget et de la Direction générale de la CSDM. Tous les frais liés aux dispositifs technologiques et aux travaux nécessaires à l'implantation de ces restrictions seront cependant à la charge de l'unité requérante.
- Le gestionnaire doit formuler par écrit toute demande concernant les activités de surveillance et de contrôle d'accès précitées et les adresser à l'intention du gestionnaire désigné à cet effet par le SGPDC. C'est ce service qui est responsable de juger de la recevabilité de la demande.

Service des technologies de l'information (STI)

En matière de sécurité de l'information, le STI s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information et dans la réalisation de projets de développement ou d'acquisition dans lesquels il intervient.

Le STI :

- Doit élaborer une stratégie concernant la sécurité de l'information à la CSDM.
- Doit mettre en place une structure permettant l'évaluation régulière de sa stratégie de sécurité et doit effectuer les corrections nécessaires à son bon fonctionnement.
- Doit participer activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre ainsi qu'à l'anticipation de toute menace en matière de sécurité des systèmes d'information numériques faisant appel aux technologies de l'information.
- Doit appliquer des mesures de réaction appropriées à toute menace ou incident de sécurité de l'information, tel que, par exemple, l'interruption ou la révocation temporaire, lorsque les circonstances l'exigent, des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause.
- Doit participer à l'exécution des enquêtes autorisées par la direction générale relativement à des contraventions réelles ou apparentes à la présente Directive.
- Est responsable de la mise à jour de la **Directive de sécurité** et de son cadre de gestion.

Le STI est responsable du bon fonctionnement du parc informatique de la CSDM, qui regroupe l'ensemble des outils technologiques et des infrastructures mis à la disposition des utilisateurs. Des règles déontologiques et éthiques particulières s'appliquent à certaines catégories de personnel du STI : c'est le cas du personnel responsable des infrastructures et des applications institutionnelles (annexe II) ainsi que du personnel de soutien informatique (annexe III).

Le STI :

- Doit élaborer une stratégie concernant l'utilisation des technologies à la CSDM.
- Doit mettre en place une structure permettant l'évaluation régulière de sa stratégie concernant l'utilisation des technologies et doit effectuer les corrections nécessaires à son bon fonctionnement.
- Doit réaliser les enquêtes concernant le comportement des utilisateurs, à la demande du SGPDC.
- Peut amorcer, sans autorisation préalable, une enquête visant à cibler ou à qualifier des comportements spécifiques ou des habitudes de groupes d'utilisateurs au regard des outils et des infrastructures technologiques, à des fins de vérification, de documentation ou de sensibilisation des utilisateurs.
- Est responsable de rendre compte à la CSDM des tendances qui concernent le comportement des utilisateurs, contribuant ainsi à la sensibilisation requise en ce qui a trait à une utilisation éthique et conforme des outils et infrastructures technologiques.
- Est responsable d'autoriser l'attribution des droits d'administration d'un utilisateur après discussion entre le gestionnaire responsable des infrastructures informatiques de la CSDM et le gestionnaire concerné ou encore de révoquer de tels droits lorsque les tâches caractéristiques de l'utilisateur ne répondent pas aux critères donnant accès aux droits d'administration, tels qu'ils sont prévus dans les **Lignes directrices d'utilisation**.
- Doit déterminer les balises d'accès aux infrastructures technologiques de la CSDM, notamment les privilèges d'accès élevés, tels que l'accès par lien RPV (annexe IV).
- Est responsable de la mise à jour des **Lignes directrices d'utilisation** et de son cadre de gestion.
- Doit conseiller, de pair avec le SGPDC, les gestionnaires de la CSDM pour tout sujet qui concerne les **Lignes directrices d'utilisation**.

Service des ressources matérielles (SRM)

Le SRM participe, avec le RSI et les CSGI à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels de la CSDM.

Service de la gestion des personnes et du développement des compétences (SGPDC)

Le SGPDC, en vertu de sa fonction de conseil auprès des gestionnaires de la CSDM, assume des responsabilités spécifiques au regard de la Directive de sécurité et des **Lignes directrices d'utilisation** ainsi que des gestes à poser visant leur application.

Le SGPDC :

- Doit s'assurer d'intégrer à ses processus d'embauche et de recrutement une communication claire qui concerne la Directive de sécurité et les **Lignes directrices d'utilisation** ainsi que les responsabilités qui en découlent pour l'employé.
- Doit s'assurer que tout nouvel employé de la CSDM soit avisé de la Directive de sécurité et des **Lignes directrices d'utilisation** et obtenir son engagement au respect de cette Directive et des Lignes directrices.

- Doit exercer un rôle-conseil auprès des gestionnaires quant à l'encadrement des utilisateurs au regard de leur utilisation des outils technologiques.
- Doit désigner un gestionnaire responsable de recevoir les demandes de contrôle, de vérification ou de surveillance de l'utilisation.
- Doit autoriser toute demande d'un gestionnaire de la CSDM visant le contrôle, la vérification ou la surveillance active des activités d'un utilisateur ou d'un groupe d'utilisateurs.

Détenteur de l'information

Le détenteur de l'information est le gestionnaire détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif, et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il peut donc y avoir plusieurs responsables d'actifs informationnels dans une commission scolaire. Le responsable d'actifs informationnels peut déléguer la totalité ou bien une partie de sa responsabilité à un autre membre du service.

Le détenteur de l'information :

- Doit informer le personnel relevant de son autorité et les tiers avec lesquels transige son service de la Directive sur la sécurité de l'information et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer.
- Doit collaborer activement à la catégorisation des actifs informationnels du service sous sa responsabilité et à l'analyse de risques.
- Doit voir à la protection des actifs informationnels et des systèmes d'information sous sa responsabilité et veiller à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la Directive de sécurité de l'information et de tout autre élément du cadre de gestion.
- Doit s'assurer 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 voir à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion.
- Doit rapporter au CSGI toute menace ou tout incident afférant à la sécurité de l'information.
- Doit collaborer 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 et non numériques.
- Doit rapporter au CSGI tout problème lié à l'application des présentes Directives, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de ces Directives.

Utilisateurs

Tout utilisateur de la CSDM doit se conformer aux lois, aux politiques et aux directives en vigueur dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels ou utilise des outils technologiques.

Veuillez vous référer au document « ***Glossaire de la sécurité de l'information et de l'utilisation des technologies à la Commission scolaire de Montréal*** » pour plus de détails et au « **Guide de nomination** » pour une liste détaillée des rôles et responsabilités en sécurité de l'information.

8. SENSIBILISATION ET FORMATION

La sécurité de l'information et l'utilisation adéquate des technologies reposent sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté de la CSDM doivent être formés et sensibilisés :

- À la sécurité de l'information et des systèmes d'information de la CSDM.
- Aux directives de la sécurité.
- À la gestion des risques et des incidents.
- Aux menaces existantes.
- Aux conséquences d'une atteinte à la sécurité.
- Aux comportements attendus pour l'utilisation des technologies à la CSDM.
- À leur rôle, droits, responsabilités et obligations en matière de sécurité et d'utilisation.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. De plus, des documents explicatifs sont disponibles sur le site Internet de la CSDM.

9. DIFFUSION ET MISE À JOUR

Le RSI, assisté du Directeur général, est responsable de la diffusion et de la mise à jour du cadre de gestion. Le cadre de gestion sera révisé périodiquement selon les mises à jour effectuées.

10. ENTRÉE EN VIGUEUR

Le présent **cadre de gestion de la sécurité de l'information et de l'utilisation des technologies** entre en vigueur à la date de son adoption par le Conseil des commissaires.

Commission scolaire de Montréal

ANNEXE I - DÉCLARATION D'ENGAGEMENT DES UTILISATEURS

Déclaration d'engagement par les utilisateurs quant au respect des règles de sécurité de l'information et de l'utilisation des technologies

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par la CSDM et de les utiliser de façon responsable.

À cette fin, ils doivent :

- ✓ Se conformer aux directives de la CSDM, à la Directive sur la sécurité de l'information, à la Directive sur l'utilisation des technologies, ainsi qu'aux directives sectorielles, aux procédures et aux autres lignes de conduite se rapportant à la sécurité de l'information et à l'utilisation des technologies à la CSDM.
- ✓ 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.
- ✓ Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier la configuration des mesures de sécurité ou les désactiver.
- ✓ Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister.
- ✓ Utiliser uniquement leur propre code utilisateur pour accéder aux outils technologiques mis à leur disposition par la CSDM.
- ✓ Utiliser les outils technologiques de façon responsable en priorité selon les besoins reliés à leurs fonctions.
- ✓ Limiter l'utilisation personnelle des outils technologiques afin qu'elle ait lieu en dehors des heures de travail et ne nuise pas à l'efficacité ou à la disponibilité des systèmes informatiques.
- ✓ Respecter la confidentialité des communications qu'ils reçoivent et signifier clairement le caractère confidentiel des communications qu'ils émettent.
- ✓ Accéder au réseau interne de la CSDM uniquement selon les diverses règles établies concernant l'utilisation des outils technologiques sur les réseaux filaires, sans fil ou par lien SSL-RPV (VPN).
- ✓ Accepter que les outils technologiques mis à leur disposition par la CSDM soient administrés à distance sans qu'ils puissent eux-mêmes disposer de droits d'administration sur ces outils.
- ✓ Signaler immédiatement à leur supérieur tout acte dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la CSDM.
- ✓ Remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout outil technologique qui avaient été mis à leur disposition dans le cadre de l'exercice de leurs fonctions, au moment de leur départ de la CSDM.

Je, soussigné(e), _____, reconnais avoir pris connaissance des règles, ci-dessus reproduites, sur la sécurité de l'information et l'utilisation des technologies de la CSDM et m'engage à les respecter. Avant d'apposer ma signature, j'ai lu les annexes III et IV et pris connaissance des règles et responsabilité qui s'appliquent.

Signature :_____ Date : _____

ANNEXE II - RÈGLES POUR LE GESTIONNAIRE INFORMATIQUE

Règles d'éthique et de déontologie s'adressant au gestionnaire des infrastructures informatiques de la CSDM et au personnel auquel il délègue certaines tâches

La direction du Service des technologies de l'information est le gestionnaire principal des infrastructures informatiques de la CSDM. À ce titre, elle est responsable et répondante des actions entreprises par son service. Afin d'assurer le bon fonctionnement des infrastructures, il délègue des responsabilités de gestion aux cadres de son service qui gèrent les réseaux, les systèmes, les applications institutionnelles et les ressources humaines responsables des opérations.

Dans le cadre de l'exercice de ses responsabilités, et uniquement dans ce contexte, le gestionnaire des infrastructures jouit de privilèges qui lui permettent de demander l'exécution de certaines actions dans le but d'assurer le bon fonctionnement des systèmes sous sa responsabilité ainsi que le respect des règles générales d'utilisation. Le gestionnaire des infrastructures doit toutefois s'assurer d'être en mesure de justifier les gestes qu'il peut poser.

À cet égard, un membre du personnel du STI qui doit exécuter ces actions à la demande du gestionnaire des infrastructures :

- Peut jouir de privilèges d'accès supérieurs à ceux du simple utilisateur, selon les besoins de sa tâche.
- Peut contrôler l'accès et l'utilisation des systèmes sous sa responsabilité et utiliser les données d'administration produites par ces systèmes afin de remplir ses obligations.
- Peut accéder aux données des utilisateurs dans le but d'effectuer l'entretien ou d'optimiser la performance des systèmes, d'en assurer la sécurité ou dans le but de vérifier la conformité du comportement d'un utilisateur en regard des attentes de la CSDM à son endroit.
- Peut prendre des copies de sécurité des données des utilisateurs.
- Peut surveiller le traitement et la transmission des données.
- Peut arrêter et réamorcer un système.
- Peut contrôler les ressources d'un système.
- Peut dépister des brèches de sécurité, y compris les mots de passe trop faciles à découvrir et empêcher l'accès des personnes qui ne font plus partie du personnel de la CSDM.
- Peut prendre les moyens appropriés pour corriger une situation et modifier les droits d'accès d'un utilisateur si le gestionnaire des infrastructures a des motifs de croire que l'utilisateur concerné contrevient aux règles générales d'utilisation ou à la Directive d'utilisation.

ANNEXE III - RÈGLES POUR LE PERSONNEL DE SOUTIEN INFORMATIQUE

Règles d'éthique et de déontologie s'adressant au personnel responsable du soutien informatique

Ces règles d'éthique et de déontologie énoncent des principes qui doivent guider les actions du personnel responsable du soutien informatique, tant dans l'application des **Lignes directrices d'utilisation** et des règlements de la CSDM que lorsque surviennent des situations pour lesquelles rien de spécifique n'est prévu. Même si ces règles visent à fournir un guide d'action et de réflexion, elles ne peuvent, évidemment, couvrir toutes les situations. Il revient donc à chacun de faire preuve de jugement et d'agir de façon responsable en appliquant ces principes dans son vécu quotidien et en demandant de l'aide au besoin. En cas de doute, il convient de se référer à son supérieur immédiat et de se questionner à savoir si ses actions s'inscrivent dans le cadre des valeurs et principes de la Directive d'utilisation, de la mission de la CSDM et du respect des utilisateurs.

Ces règles d'éthique et de déontologie visent les employés, les stagiaires et les fournisseurs de service ayant comme mandat principal le soutien informatique, qu'ils fassent partie du personnel du STI ou qu'ils dépendent de tout autre service, établissement ou organisme. Cette responsabilité comporte certains privilèges et conséquemment certaines exigences, certains devoirs, que chacun s'engage à respecter dans ses gestes professionnels.

1. Le respect des personnes

La mise en place et l'utilisation d'outils technologiques ont un effet sur la vie professionnelle ou personnelle des utilisateurs, que ce soit par la modification des méthodes de travail, les changements aux moyens de communication, la transformation des équipes ou simplement la conservation de données à leur sujet. Le respect des personnes devient donc une valeur fondamentale pour les intervenants. Ainsi, il importe de mettre en œuvre les moyens permettant d'éviter de nuire aux personnes par suite soit de l'implantation d'outils technologiques, soit de la divulgation, volontaire ou non, d'informations confidentielles, soit de dysfonctions causant des pertes, soit encore de la possibilité d'utiliser les systèmes mis à la disposition des utilisateurs de façon à nuire à quelqu'un.

Ce respect des personnes doit également se traduire dans les relations entre les membres du personnel de soutien informatique en accordant le crédit aux collaborateurs pour leurs travaux et en partageant ses connaissances pour aider ses collègues à obtenir de meilleurs résultats.

2. L'attitude PAR RAPPORT aux utilisateurs

L'attitude des membres du personnel de soutien informatique par rapport à ces derniers doit en être une d'ouverture, de franchise, d'honnêteté et de respect. Devant un choix mettant en contradiction la satisfaction des besoins des utilisateurs et la facilité pour l'informaticien, en général et sous réserve de contraintes financières ou techniques, le premier prévaudra afin de viser la satisfaction de la clientèle.

3. Le respect des normes et des règles de l'art

Nonobstant les objectifs de service à la clientèle, les actions de soutien sont balisées par les diverses normes et règlements applicables à la CSDM. Le personnel de soutien informatique doit ainsi connaître les **Lignes directrices d'utilisation** et y adhérer, de même qu'il doit se référer aux bases de connaissances à sa disposition ainsi qu'aux normes édictées par le Service des technologies de l'information pour définir son champ d'action. Le personnel de soutien informatique doit en outre être en mesure d'expliquer les normes aux utilisateurs, ou encore de faire valoir des modifications qui pourraient être apportées à ces normes, dans une perspective d'amélioration du service.

Le personnel de soutien informatique est également responsable, en première ligne, du respect des normes s'appliquant aux utilisateurs. À ce titre, il doit intervenir pour toute situation de non-conformité, d'abord auprès de l'utilisateur concerné, puis auprès du gestionnaire de l'unité concernée. Lorsque la situation de non-conformité persiste malgré ses interventions, le personnel de soutien informatique doit en aviser son supérieur immédiat.

En outre, il est du devoir d'un membre du personnel de soutien informatique de connaître et de respecter les lois, les règlements et les bonnes pratiques qui encadrent ses actions, et d'être à l'affut des développements dans son domaine d'expertise.

4. L'intégrité et l'honnêteté

L'intégrité et l'honnêteté forment la base de la confiance. Elles s'appliquent tant dans l'utilisation des outils que dans l'accès aux données personnelles, l'installation de logiciels qui pourraient être illicites, le respect de la propriété intellectuelle et le comportement général des personnes.

Ainsi, tout membre du personnel de soutien informatique :

- Doit conserver le secret sur tout renseignement confidentiel obtenu en cours de mandat.
- Ne doit pas utiliser de données confidentielles à des fins personnelles.
- Doit éviter tout conflit d'intérêts ou favoritisme.
- Doit être responsable des décisions et des gestes posés dans le cadre de son travail et être imputable de ses actions.
- Ne doit utiliser les ressources appartenant à la CSDM que dans le contexte autorisé.
- Doit respecter la Loi sur le droit d'auteur, en particulier au sujet des copies illicites de logiciels, du dévoilement de secrets commerciaux et de la violation de conditions de licences des produits en usage.
- Doit sensibiliser les utilisateurs aux mesures de sécurité relatives à l'intégrité des outils technologiques et à l'utilisation du cyberespace.
- Doit établir et faire connaître les risques et limitations des technologies.

5. Les responsabilités PAR RAPPORT aux élèves

En toute concordance avec la mission première de la CSDM, le personnel de soutien informatique doit contribuer à ce que les outils technologiques mis à la disposition des élèves favorisent leur réussite éducative. Notamment, il doit promouvoir auprès des élèves et des autres utilisateurs des pratiques sécuritaires dans l'utilisation des outils technologiques au regard des enjeux suivants :

- La protection de leur identité
- La détermination de menaces à la sécurité ou à l'intégrité de leurs outils technologiques
- Le cybercivisme
- Le respect des droits de propriété intellectuelle et le logiciel libre

ANNEXE IV - ACCÈS DISTANT AU RÉSEAU DE LA CSDM

Balises pour l'accès distant au réseau de la CSDM par l'entremise d'un réseau privé virtuel sécurisé (SSL-RPV)

Ce document établit les balises devant guider la gestion des accès par SSL-RPV au réseau interne de la CSDM et leur utilisation. Ces balises doivent être respectées par quiconque souhaite bénéficier d'un accès par SSL-RPV au réseau interne de la CSDM.

1. Principe directeur

L'accès au réseau interne de la CSDM par voie d'un lien SSL-RPV est un privilège réservé aux quelques personnes au sein de la CSDM qui doivent accéder, de leur domicile ou d'un lieu hors de la portée du réseau interne de la CSDM, à des ressources du réseau interne auxquelles on ne peut accéder par d'autres voies. C'est notamment le cas des applications institutionnelles de la CSDM qui ne disposent pas d'une interface Web.

Pour la grande majorité des employés et des collaborateurs de la CSDM, les outils Web permettant d'accéder aux applications institutionnelles, aux outils de communication ou aux espaces de stockage constituant l'infrastructure technologique de la CSDM suffisent à leurs besoins d'accès distant.

2. Demande d'accès SSL-RPV

Toute personne souhaitant accéder au réseau interne de la CSDM par voie d'un accès SSL-RPV :

- Doit être l'utilisateur d'un ordinateur portable de technologie PC propriété de la CSDM et configuré pour un accès au segment administratif du réseau interne de la CSDM.
- Doit remplir un formulaire de demande d'accès SSL-RPV (formulaire R105).

Aucuns frais ne sont associés à l'utilisation d'un accès par SSL-RPV.

3. Responsabilités du Service des technologies de l'information (STI)

Le STI est responsable des actions suivantes :

- Configurer l'ordinateur du requérant pour permettre un accès distant par SSL-RPV.
- Remettre à l'utilisateur la documentation requise pour l'utilisation de l'accès.
- S'assurer de la continuité du service pour l'ensemble des utilisateurs.

4. Responsabilités de l'utilisateur

- L'utilisateur est responsable de gérer tous les aspects liés à l'obtention d'un accès distant par SSL-RPV. De plus, il doit s'assurer de disposer à ses frais d'un accès fonctionnel à Internet à partir du fournisseur de services de son choix.
- L'utilisateur disposant de privilèges d'accès par SSL-RPV doit s'assurer qu'aucune autre personne et qu'aucun autre poste de travail, incluant tout ordinateur personnel appartenant à l'utilisateur, ne peut accéder au réseau par le lien SSL-RPV qui lui a été accordé.
- L'utilisateur dont le poste portable est lié au réseau interne de la CSDM par lien SSL-RPV doit comprendre qu'il est soumis à toutes les dispositions de la Directive d'utilisation.
- L'utilisation du lien SSL-RPV requiert que le poste portable utilisé dispose des dernières mises à jour du système d'exploitation et de l'antivirus, lesquelles sont disponibles automatiquement par l'entremise du réseau interne.

5. Retrait, révocation et transfert du privilège d'accès par SSL-RPV

- Quiconque ne respecte pas les balises établies dans le présent document verra ses privilèges d'accès révoqués temporairement ou de façon permanente, selon la situation et après discussion entre le STI et le responsable de l'unité administrative à laquelle la personne concernée est rattachée.
- Le privilège d'accès est transférable d'un utilisateur à un autre sans frais, en fonction des changements dans l'organisation du travail ou des mouvements de personnel requérant un tel transfert de privilèges. Dans un tel cas, le transfert doit être demandé par le responsable de l'unité administrative concernée.
- Tout privilège d'accès au réseau par SSL-RPV pourra être retiré à l'utilisateur concerné lorsque le lien ne sera pas utilisé pour une période de un (1) an.

6. Autres considérations

- L'utilisateur ne doit pas lier le poste portable réservé au lien SSL-RPV à un réseau d'échange de fichiers (peer to peer), à un groupe résidentiel ou à toute autre forme de réseau local.
- L'établissement d'un lien SSL-RPV à partir d'un poste portable partagé par plusieurs utilisateurs n'est pas permis, sauf dans le cas explicite où une entente à cet effet aurait été conclue entre l'unité administrative concernée et le Service des technologies de l'information.
- La gestion du dossier de l'accès par lien SSL-RPV est confiée au Bureau des infrastructures et du centre de services (BICS) du Service des technologies de l'information.
- Toute dérogation aux balises décrites dans le présent document doit faire l'objet d'une entente officielle entre le STI et l'unité administrative concernée.

Commission scolaire de Montréal

Lignes directrices sur l'utilisation des technologies

Direction générale de la Commission scolaire de Montréal

Cette page est laissée vide intentionnellement

Commission scolaire de Montréal

HISTORIQUE

Auteur	Rôle	Description	Date
Daniel Martin	Directeur adjoint du STI	• Création du document original	2014-06-18
Guy Nicol	Analyste au STI	• Transfert des sections sécurité et droits d'auteurs vers la Directive de sécurité	2019-03-13
Guy Nicol	Analyste au STI	• Réorganisation	2019-03-14 au 2019-03-25
Guy Nicol	Analyste au STI	• Uniformisation	2019-03-26 au 2019-05-02
Guy Nicol Comité de sécurité Sylvie Gallant	Analyste au STI Membres de comité de sécurité Secrétaire générale	• Révision finale	2019-05-03 au 2019-06-13

Commission scolaire de Montréal

TABLE DES MATIERES

1. PRÉAMBULE

Le document ***Lignes directrices sur l'utilisation des technologies à la Commission scolaire de Montréal (CSDM)***, ci-après nommé ***Lignes directrices d'utilisation***, remplace et complète le ***Code d'éthique sur l'utilisation des technologies de l'information et des communications et des équipements informatiques à la CSDM***. Les ***Lignes directrices d'utilisation*** s'adressent à quiconque utilise des outils technologiques dans le cadre de ses fonctions ou de ses activités à la CSDM. Elles définissent, d'une part, les comportements attendus des utilisateurs ainsi que les mécanismes de contrôle visant le respect de ces comportements attendus. D'autre part, elles visent à définir les principes directeurs qui doivent baliser l'intégration des technologies dans le cadre des différentes activités qui ont cours à la CSDM : l'apprentissage et l'enseignement, l'administration, les communications interpersonnelles, les jeux et loisirs; bref, toute activité médiatisée par une technologie.

Les ***Lignes directrices d'utilisation*** sont par ailleurs subordonnées à toute loi, convention ou politique et à tout règlement pouvant baliser le comportement des utilisateurs et des personnes responsables de son application, de même que leurs choix technologiques.

Enfin, les ***Lignes directrices d'utilisation*** accompagnent la Directive sur la sécurité de l'information et sont complétées par un cadre de gestion.

2. DÉFINITIONS

Les diverses définitions utilisées dans ce document sont expliquées plus en détail dans le ***Glossaire de la sécurité de l'information et de l'utilisation des technologies à la commission scolaire de Montréal***.

3. CHAMP D'APPLICATION

Les ***Lignes directrices d'utilisation*** s'appliquent en tout temps à tous les utilisateurs, c'est-à-dire à toute personne qui utilise directement ou indirectement les outils technologiques et l'infrastructure technologique de la CSDM.

4. PRINCIPES DIRECTEURS

En toute concordance avec les valeurs communes et les principes directeurs énoncés par la ***Déclaration de principes sur le civisme et l'éthique à la CSDM***, l'intégration des technologies à la CSDM, tant sur le plan du comportement des utilisateurs que de la gestion des outils technologiques, doit obéir aux principes directeurs suivants :

4.1. Respect des personnes

L'utilisation des technologies à la CSDM doit prendre en compte les valeurs de respect et de considération essentielles au vivre-ensemble. L'expression de ces valeurs doit être visible dans les diverses communications de l'utilisateur, tant par le contenu que par la qualité du français écrit ou oral.

4.2. Ouverture

En reconnaissance de l'évolution continue des technologies et de l'apport potentiel de ces technologies à l'apprentissage et à l'enseignement de même qu'à la réalisation des différentes fonctions au sein de la CSDM, Les ***Lignes directrices d'utilisation*** doivent témoigner d'une ouverture à l'innovation, notamment en ce qui concerne le recours aux réseaux sociaux, l'accès à l'information sur le Web et la considération du logiciel libre pour tout nouveau projet technologique.

4.3. Responsabilité

Comme les outils technologiques permettent une vaste gamme d'actions publiques, dont la communication interne et externe de même que la production et la diffusion de contenus, chaque utilisateur doit être conscient qu'il est responsable en toutes circonstances de ses productions et communications, de même que des conséquences de celles-ci. En outre, le respect des ***Lignes directrices d'utilisation*** relève d'une responsabilité individuelle et collective, en toute cohérence avec la mission de la CSDM.

4.4. Imputabilité

L'utilisateur est imputable de son utilisation des outils technologiques et du respect des Lignes directrices d'utilisation. Ce principe d'imputabilité comporte l'obligation pour l'utilisateur de s'approprier les présentes ***Lignes directrices d'utilisation*** et de tendre à un comportement éthique en ce qui concerne le recours aux technologies de l'information dans le cadre de ses fonctions. En contrepartie, la CSDM doit, par des actions de formation, d'information et de sensibilisation, favoriser le développement de cette expertise éthique chez l'utilisateur.

En reconnaissance du principe d'imputabilité tel qu'il a été défini précédemment, toute forme de comportement non conforme aux présentes ***Lignes directrices d'utilisation*** expose l'utilisateur à des sanctions qui pourront être déterminées en fonction de la nature du manquement, de sa gravité, de son impact sur le bon fonctionnement de la CSDM ou de sa chronicité.

4.5. Propriété des données

Toute donnée produite par un utilisateur dans le cadre de ses fonctions et stockée dans un outil informatique appartenant à la CSDM ou au sein d'une infrastructure hébergée à la demande de la CSDM à l'extérieur de son réseau appartient en propre à la CSDM. La CSDM se réserve ainsi le droit d'accéder à ce contenu sans l'autorisation de l'utilisateur. En contrepartie, la CSDM s'engage à faire preuve de la plus grande réserve dans l'exercice de ce droit et à limiter cet accès aux situations qui le requièrent pour des motifs de sécurité informatique, de vérification ou d'enquête selon des modalités clairement définies, notamment lorsqu'elle a des motifs raisonnables de croire en une utilisation abusive des outils technologiques mis à la disposition de l'utilisateur ou contraire aux présentes ***Lignes directrices d'utilisation***.

4.6. Efficience

La CSDM vise une utilisation efficiente de ses investissements informatiques : le recours aux technologies s'inscrit donc dans une recherche de productivité ou de profitabilité pour toutes les activités de la CSDM, tant sur le plan pédagogique qu'administratif, et ce, en considérant les coûts d'acquisition et d'exploitation des outils technologiques demandés par les utilisateurs.

5. DROITS, RESPONSABILITÉS ET OBLIGATIONS DE L'UTILISATEUR

L'utilisation des technologies à la CSDM requiert de la part de tout utilisateur le respect des responsabilités et obligations qui suivent :

5.1. Identification

L'utilisateur doit établir son identité s'il souhaite utiliser un outil informatique sur le réseau interne de la CSDM. Pour ce faire, il utilise son code utilisateur et le mot de passe qui lui est propre.

Conséquemment, l'utilisateur est responsable de préserver la confidentialité de son mot de passe. Il ne doit le divulguer à personne, pas même à ses supérieurs. Dans le cas où une divulgation du mot de passe est requise pour des motifs liés au soutien informatique, l'utilisateur doit immédiatement le modifier après la divulgation. Aussi, la CSDM doit fournir un code utilisateur et un mot de passe personnel à tout utilisateur capable de s'en servir pour accéder à un outil technologique ou à un élément de l'infrastructure technologique de la CSDM.

En clair, l'utilisateur est responsable de toute utilisation de son code utilisateur et de son mot de passe : il doit considérer son code utilisateur et son mot de passe comme sa signature.

5.2. Adhésion aux *Lignes directrices d'utilisation*

Tout utilisateur doit adhérer explicitement aux présentes ***Lignes directrices d'utilisation*** et s'engager, dans les limites de sa compréhension, à en respecter l'esprit et la lettre. Tout utilisateur doit donc prendre connaissance des ***Lignes directrices d'utilisation*** et du

cadre de gestion en découlant qui sont établis par la CSDM. En contrepartie, la CSDM doit mettre en place les mécanismes permettant une adhésion explicite pour tous les utilisateurs, de même qu'elle doit faire en sorte que les présentes ***Lignes directrices d'utilisation*** soient connues et comprises par ceux-ci.

La Commission scolaire pourra notamment demander à tout utilisateur de confirmer qu'il a pris connaissance des ***Lignes directrices d'utilisation*** et qu'il s'engage à les respecter.

5.3. Utilisation responsable des outils technologiques de la CSDM

L'utilisation de tout outil technologique, incluant l'accès à Internet, doit être réservée en priorité aux besoins liés à la fonction. Également, les restrictions et devoirs suivants s'appliquent :

5.3.1. L'utilisateur s'engage à utiliser les équipements mis à sa disposition de façon consciencieuse, efficace et responsable.

5.3.2. L'utilisateur se sert des outils technologiques de la CSDM en toute connaissance du fait qu'ils sont rattachés à sa fonction et non à lui personnellement.

5.3.3. L'utilisateur est responsable de prendre les mesures nécessaires, au meilleur de ses connaissances, afin de protéger le bon fonctionnement et l'intégrité des outils technologiques dont il dispose.

5.3.4. Pour tous les outils technologiques mobiles, l'utilisateur est responsable en tout temps de l'utilisation qui en est faite et doit en limiter les accès afin d'en assurer la sécurité. Il doit en outre adopter des comportements qui minimiseront les risques de bris ou de vol.

5.3.5. L'utilisateur ne doit pas faire usage des outils technologiques mis à sa disposition par la CSDM à des fins commerciales, publicitaires ou militantes, exception faite d'actions demandées par la CSDM ou d'actions qui reflètent la nature politique de la fonction occupée ou du rôle exercé au sein de la CSDM.

5.3.6. L'utilisateur s'engage à ne pas utiliser de manière illicite ou inappropriée le réseau interne ou les autres outils technologiques mis à sa disposition par la CSDM. On entend par « illicite ou inapproprié » la visite de sites, l'envoi ou la réception de contenus de nature haineuse, discriminatoire, indécente, pornographique, raciste, violente, illégale ou incitant à des comportements de cette nature, de même que tout comportement de cyberintimidation.

5.3.7. L'utilisateur doit s'abstenir de tout téléchargement qui n'a pas de lien avec ses tâches caractéristiques et qui pourrait compromettre le bon fonctionnement de ses outils informatiques.

5.3.8. La consommation de contenu radiophonique ou télévisuel en téléchargement continu (streaming) n'ayant pas de lien avec les tâches caractéristiques de l'utilisateur lors des heures de travail est proscrite, sauf à des fins pédagogiques ou de développement professionnel.

5.4. Droit d'utilisation à des fins personnelles

L'utilisation des outils technologiques fournis par la Commission scolaire à des fins personnelles est permise, à titre de privilège, pour autant qu'aucun doute ne soit émis quant à l'incidence de cette utilisation personnelle sur les tâches qui incombent à l'utilisateur. En outre, l'utilisateur doit respecter les dispositions des ***Lignes directrices d'utilisation*** et du cadre de gestion déterminées par la CSDM lorsqu'il fait usage d'outils technologiques de la CSDM ou lorsqu'il sollicite les ressources de l'infrastructure technologique de la CSDM à des fins personnelles.

Les conditions d'utilisation personnelle attendues sont les suivantes :

- L'utilisation personnelle doit se situer en dehors des heures habituelles de prestation de travail.
- L'utilisation personnelle ne nuit nullement aux opérations de la Commission scolaire, ni à l'efficacité ou à la disponibilité des systèmes informatiques.
- La durée de l'utilisation personnelle est limitée et ne peut être assimilée à du cyberflânage.

5.5. Droit au respect du caractère privé de certaines communications

La CSDM reconnait le caractère privé de certaines communications faites avec les outils informatiques lui appartenant, notamment les communications de nature purement personnelle, syndicale ou associative, de même que les communications ayant trait à des informations à caractère confidentiel. Pour toutes ces situations, l'utilisateur doit signifier à ses interlocuteurs le caractère confidentiel ou privé de la communication produite. En contrepartie, l'utilisateur qui reçoit une communication à caractère confidentiel lui étant destinée doit en respecter le caractère confidentiel et s'engager à ne pas diffuser, transférer ou dévoiler de quelque manière que ce soit cette information sans l'autorisation explicite de son interlocuteur.

5.6. Droit spécifique d'accès au réseau interne de la CSDM

L'utilisateur peut accéder au réseau interne de la CSDM par voie filaire, c'est-à-dire par le branchement d'un outil technologique à une prise réseau située dans un bâtiment de la CSDM, par sans-fil (wifi), c'est-à-dire par l'intermédiaire d'un signal émis par une borne sans fil connectée au réseau filaire de la CSDM, ou encore par lien SSL-RPV. Des droits spécifiques s'appliquent à chacune de ces connexions.

5.6.1. Seuls les outils technologiques appartenant à la CSDM et répondant aux critères établis à cet effet par le responsable de ses infrastructures informatiques peuvent bénéficier d'un branchement filaire au réseau interne de la CSDM.

5.6.2. Certains des outils technologiques appartenant à la CSDM peuvent également bénéficier d'un accès sans fil au réseau interne.

5.6.3. Les outils technologiques appartenant à l'utilisateur interne ou requis par un utilisateur externe peuvent être liés au réseau sans fil de la CSDM sans autorisation du responsable de ses infrastructures informatiques seulement si un réseau pour

invités ou visiteurs est disponible à l'endroit où l'utilisateur souhaite se brancher. Toute autre forme de branchement est interdite.

5.6.4. Si le branchement d'un utilisateur externe au réseau filaire de la CSDM s'avère nécessaire aux activités de la CSDM, une autorisation préalable du responsable de ses infrastructures informatiques doit être sollicitée.

5.6.5. Le recours à un branchement par lien RPV requiert une autorisation du responsable des infrastructures informatiques de la CSDM, de même que des conditions spécifiques d'acceptation de service définies à l'intérieur du cadre de gestion des présentes ***Lignes directrices d'utilisation***.

5.7. Droit d'administration des outils informatiques

L'utilisateur dispose d'un droit d'administration lorsqu'il peut, sans l'aide ou sans l'autorisation des services de soutien informatique, installer des logiciels ou modifier les paramètres de fonctionnement d'un outil informatique. Or, sauf exception, l'utilisateur interne ne doit pas disposer des droits d'administration complets pour tout outil mis à sa disposition par la CSDM.

Les exceptions suivantes s'appliquent :

- Le personnel responsable des technologies de l'information de la CSDM et requérant, par ses fonctions, un droit d'administration.
- Le personnel de soutien informatique au plan de l'effectif d'une autre unité de la CSDM.
- Un utilisateur dont la principale fonction, telle qu'elle est reconnue par un gestionnaire concerné, consisterait à soutenir l'intégration des technologies à la fonction.

L'utilisateur interne peut toutefois être administrateur d'un téléphone cellulaire ou d'une tablette numérique iPad, sous réserve du respect des engagements précités relatifs à une utilisation responsable des outils technologiques de la CSDM. Par ailleurs, certains droits d'administration pourraient être délégués aux utilisateurs, selon l'évolution des technologies permettant la gestion de ces droits et en fonction des orientations déterminées entièrement par le Service des TI.

5.8. Responsabilités relatives à la sécurité informatique

Les responsabilités relatives à la sécurité informatique sont définies dans la ***Directive sur la sécurité de l'information***.

5.9. Responsabilités relatives aux droits d'auteur

Les responsabilités relatives aux droits d'auteur sont définies dans la ***Directive sur la sécurité de l'information***.

5.10. Responsabilités relatives aux communications par messagerie numérique

L'utilisation de la messagerie numérique comporte d'importants bénéfices pour l'utilisateur et pour la CSDM. Cependant, certaines balises doivent être établies afin d'éviter que ces moyens de communication ne viennent compromettre la réalisation des tâches qui incombent à l'utilisateur et à ses pairs.

5.10.1. L'utilisateur s'engage à faire preuve de respect et de discernement dans ses communications et s'engage à se servir des divers types de messagerie pour des motifs justifiés par les tâches qui lui incombent.

5.10.2. L'utilisateur doit s'assurer, au meilleur de ses connaissances, de joindre des fichiers intègres et exempts de virus ou d'autres logiciels malveillants lorsqu'il fait usage des fonctions de pièce jointe.

5.10.3. L'utilisateur doit restreindre la taille des fichiers qu'il joint à ses envois.

5.10.4. L'utilisateur s'engage à utiliser avec discernement les listes de distribution pour l'envoi massif de courriels. Notamment, l'utilisateur ne doit pas utiliser les divers systèmes de messagerie numérique à la CSDM pour des motifs de promotion ou de publicité ou pour la diffusion d'informations n'ayant aucun lien avec sa tâche caractéristique.

5.10.5. L'utilisateur du courriel doit éviter le recours systématique aux envois en copie conforme (Cc) et en copie conforme invisible (Cci), ainsi que de la fonction « répondre à tous ». Comme toute adresse courriel comportant les suffixes @csdm, @edu.csdm, @csdmedu ou tout autre suffixe apparenté appartient en propre à la CSDM, l'utilisateur doit éviter d'utiliser l'adresse qui lui est attribuée par la CSDM comme identifiant personnel autrement que pour des besoins liés à la fonction occupée.

5.10.6. L'utilisateur interne qui quitte définitivement la CSDM perdra les droits d'utilisation de son adresse @csdm au plus tard 90 jours après son départ. Cependant, l'utilisateur interne en congé prolongé conserve les droits d'utilisation de son adresse @csdm, sauf avis contraire de sa part ou de la part de son supérieur immédiat.

5.11. Responsabilités relatives à l'utilisation des réseaux sociaux

La CSDM autorise les utilisateurs à recourir aux réseaux sociaux dans le cadre des activités associées à leur fonction, en reconnaissance de l'apport potentiel de ces outils à la réalisation de sa mission. Cette autorisation concerne tout autant les réseaux sociaux génériques (Facebook, Twitter et autres) que les réseaux sociaux spécifiquement prévus en soutien à l'enseignement ou à l'apprentissage. Cependant, les présentes ***Lignes directrices d'utilisation*** soulignent que les attentes exprimées par la CSDM par voie de sa ***Déclaration de principe sur le civisme et l'éthique*** s'appliquent au comportement des utilisateurs au sein de ces réseaux virtuels.

Aussi, la CSDM invite les utilisateurs à la plus grande diligence lorsqu'il s'agit de regrouper intervenants et élèves ou parents au sein de réseaux sociaux. La décision d'inclure un élève ou un parent au sein d'un réseau social auquel participe un intervenant doit nécessairement comporter une réflexion éthique préalable de même qu'une intention pédagogique ou communicationnelle très clairement balisée.

6. RESPONSABILITÉS ET OBLIGATIONS DES INTERVENANTS

6.1. Les gestionnaires

Les gestionnaires, dans leur ensemble, sont responsables de la mise en œuvre des ***Lignes directrices d'utilisation***, ainsi que de l'encadrement des utilisateurs. Ils doivent intervenir au besoin et peuvent demander qu'une enquête soit effectuée concernant un utilisateur ou un groupe d'utilisateurs.

6.2. Le Service de la gestion des personnes et du développement des compétences (SGPDC)

Le SGPDC est responsable de conseiller les gestionnaires concernant les ***Lignes directrices d'utilisation*** et doit s'assurer de communiquer clairement les ***Lignes directrices d'utilisation*** à l'intérieur de son processus d'embauche. Le SGPDC est aussi responsable d'autoriser les demandes d'enquêtes qui lui parviennent.

6.3. Le Service des technologies de l'information (STI)

Le STI est responsable des enquêtes et de la surveillance de l'utilisation des technologies.

6.4. La Direction générale

La Direction générale est responsable de voir à la mise en oeuvre des ***Lignes directrices d'utilisation*** et de voir à ce qu'elles soient observées par les services et établissements sous sa gouverne. La Direction générale est aussi responsable des autorisations concernant les restrictions d'accès.

6.5. Le Conseil des commissaires

Le Conseil des commissaires est responsable de l'adoption des ***Lignes directrices d'utilisation*** ainsi que d'autoriser les dérogations d'accès spécifiques pour un utilisateur ou un groupe d'utilisateurs.

7. ENTRÉE EN VIGUEUR

Les Lignes directrices d'utilisation entrent en vigueur à la date de l'adoption de la **Directive de sécurité** par le conseil des commissaires.

PRINCIPALES RÉFÉRENCES

_____ (2014), Politique concernant le Code de déontologie et d'éthique relatif à l'utilisation des technologies à la Commission scolaire de Montréal, Version approuvée par le Conseil des commissaires, Révision du 21 juin 2014.

http://ti.csdm.qc.ca/securite-informatique/code-deontologie-ethique/

_____ (2010), Code d'éthique et de déontologie, Université Laval, Direction des technologies de l'information, Révision du 18 novembre 2010 par Isabelle Langlois, chargée de communication.

www.dti.ulaval.ca/webdav/site/sit/shared/.../sit/.../code_ethique.pdf .

_____ (sans date), Code d'éthique et de déontologie du Service, Commission scolaire de la Côte-du-Sud, Service des technologies de l'information et des communications.

_____ (Coll., 2001), Code d'éthique sur l'utilisation des technologies de l'information et des communications et des équipements informatiques à la Commission scolaire de Montréal.

http://adagio/ActInfo/CdEthique/CdEthique.pdf.

_____ (2011), Politique d'utilisation des technologies de l'information et des communications à la Commission scolaire Marguerite-Bourgeoys, Commission scolaire Marguerite-Bourgeoys, Service de l'informatique.

_____ (2012), Politique relative à l'utilisation des médias sociaux, Commission scolaire de la Rivière-du-Nord, Politique no. 7110

Fillion, Stéphane (2011), Les réseaux sociaux et les relations du travail, Heenan Blaikie, conférence du 28 avril 2011 à l'ACSQ.

Trudel, Pierre et France Abran (2003), Guide pour gérer les aspects juridiques d'Internet en milieu

Commission scolaire de Montréal

Glossaire de la sécurité de l'information et de l'utilisation des technologies

Direction générale de la Commission scolaire de Montréal

Cette page est laissée vide intentionnellement

Commission scolaire de Montréal

HISTORIQUE

Auteur	Rôle	Description	Date
André Bachand	Conseiller principal de la SI – Projet SICS	• Création	2017-11-28
André Bachand	Conseiller principal de la SI – Projet SICS	• Modif déf pour CSGI, détenteur de l'information, incidents à portée gouvernementale, imputabilité, mesure de sécurité de l'information, renseignement confidentiel et RSI • Retrait déf du responsable de l'actif informationnel	2018-03-20
Lucie Perreault et comité de sécurité	Directrice du STI Resp. Sécurité de l'information	• Adaptation pour la CSDM	2019-01-14
Guy Nicol	Analyste au STI	• Intégration du glossaire de la Directive sur l'utilisation des technologies • Ajouts au glossaire	2019-03-18 au 2019-03-25
Guy Nicol	Analyste au STI	• Uniformisation	2019-03-26 au 2019-05-02
Guy Nicol Comité de sécurité Geneviève Laurin Sylvie Gallant	Analyste au STI Membres du comité de sécurité Coordonnatrice du bureau des affaires juridiques Secrétaire générale	• Révision finale	2019-05-03 au 2019-06-13

Commission scolaire de Montréal

TABLE DES MATIERES

Commission scolaire de Montréal

Définitions :

ACTIF INFORMATIONNEL

Tout actif sur lequel repose des données numériques ou non numériques.
Exemples : Base de données sur un serveur, un document papier dans un classeur.

Information, banque d'information, système ou support d'information, document, technologie de l'information, installation ou ensemble de ces éléments acquis ou constitués par la CSDM qui peuvent être accessibles avec un dispositif des technologies de l'information (logiciels, progiciels, didacticiels, banques de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale) ou accessibles par un dispositif plus traditionnel tel une filière ou un classeur.

Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

Actif informationnel numérique

Toute information stockée dans un format numérique sur un de ces médias : disque, base de données, disquette, ruban magnétique, cassette, clé USB, mémoire flash, vidéo, photo numérique, ordinateur portable, ordinateur de table, tablettes, téléphone intelligent, etc.

L'information sur le média de l'actif numérique peut être écrite, effacée, réécrite, cryptée et copiée.

Actif informationnel non numérique

Toute information autre que numérique telle : papier, microfilm, pellicule, photo papier, etc.

- L'information sur le média de l'actif non numérique, une fois produite, ne peut être effacée, réécrite, cryptée et copiée.
- Les actifs non numériques peuvent se retrouver dans une pièce, sur un mur, dans un classeur, dans une valise, dans un sac à dos, etc.
- Les actifs non numériques peuvent être facilement déplacés.
- Les actifs non numériques peuvent être produits en plusieurs copies et être à plus d'un endroit.
- Le suivi à la trace des actifs non numériques est ardu.
- Un actif non numérique qui est numérisé est considéré comme un actif numérique.
- L'information d'un actif non numérique peut varier d'une copie à une autre. Ex. : un plan d'intervention d'un élève peut être numérisé une première fois et ensuite numérisé une seconde fois quand tous les intervenants impliqués l'ont signé.

AUTHENTIFICATION

Action de permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif.

AUTORISATION

Attribution par la commission scolaire à une personne ou à un groupe de personnes d'un droit d'accès, complet ou restreint, à une information ou à un système d'information.

CADRE DE GESTION

Ensemble des consignes, politiques, règlements, directives, procédures, bonnes pratiques reconnues, comités qui encadrent les activités d'une organisation telle une commission scolaire.

CATÉGORISATION

Processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant son degré de sensibilité en matière de disponibilité, d'intégrité et de confidentialité et, par conséquent, le niveau adéquat de protection à lui accorder.

CONFIDENTIALITÉ

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

CONTINUITÉ DES SERVICES

Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

COORDONNATEUR SECTORIEL DE LA GESTION DES INCIDENTS (CSGI)

Personne nommée par le Conseil des Commissaires pour collaborer étroitement avec le COGI-réseau du MEES. Le CSGI agit aux points de vue tactique et opérationnel; il apporte le soutien nécessaire au RSI pour qu'il puisse s'acquitter de ses responsabilités et est l'interlocuteur officiel de la CSDM auprès du CERT/AQ.

Voir le ***Guide de nomination*** pour plus d'information.

CYBERCIVISME

Respect d'un utilisateur envers la collectivité dans laquelle il vit et les individus qui composent cette collectivité, comme démontré par ses actes et paroles au sein d'un réseau social ou, de manière plus générale, sur Internet, de même que le respect pour les conventions qui balisent le vivre-ensemble.

CYBERINTIMIDATION

Action de harceler une personne ou de tenir à son endroit des propos menaçants, haineux, injurieux ou dégradants, qu'ils soient illustrés ou écrits, en recourant à l'Internet ou à un outil technologique, par l'intermédiaire notamment du courriel, du clavardage, de groupes de discussion, de sites Web ou de la messagerie instantanée.

CYBERFLÂNAGE

Action d'utiliser un outil technologique à des fins qui n'ont rien à voir avec la tâche attendue de la part d'un utilisateur, élève, employé ou autre, au cours de ses heures de travail.

CYCLE DE VIE DE L'INFORMATION

Ensemble des étapes que franchit l'information, 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 de la CSDM.

DÉTENTEUR

Personne qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels de la CSDM.

DÉTENTEUR DE L'INFORMATION

Cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif, et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il peut donc y avoir plusieurs détenteurs de l'information dans une commission scolaire. Le détenteur de l'information peut déléguer la totalité ou bien une partie de sa responsabilité à un autre membre du service.

Le détenteur de l'information :

- Doit informer le personnel relevant de son autorité et les tiers avec lesquels transige le service de la **Directive de sécurité de l'information** et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer.
- Doit collaborer activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques.
- Doit voir à la protection de l'information et des systèmes d'information sous sa responsabilité et veiller à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la **Directive de sécurité de l'information** et de tout autre élément du cadre de gestion.
- Doit s'assurer 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 voir à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe

s'engage à respecter la **Directive de sécurité de l'information** et tout autre élément du cadre de gestion.
- Doit rapporter au CSGI toute menace ou tout incident numérique ou traditionnel afférant à la sécurité de l'information.
- Doit collaborer 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 de l'information.
- Doit rapporter à la direction générale tout problème lié à l'application de la **Directive de sécurité de l'information**, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de la **Directive de sécurité de l'information**.

DÉROGATION

Formulaire rempli et dûment approuvé par les intervenants appropriés permettant de déroger pour une durée de temps déterminée à un requis de sécurité après avoir identifié le risque, l'impact et la ou les mesures compensatoires.

DIRECTION GÉNÉRALE

Groupe dont le dirigeant est le premier responsable de la sécurité de l'information.

La Direction générale :
- Doit désigner les principaux intervenants en sécurité de l'information.
- Doit mettre en œuvre une directive et un cadre de gestion de la sécurité de l'information.
- Doit définir et mettre en place les processus majeurs de sécurité de l'information.
- Doit présenter régulièrement au Ministère un plan d'action et un bilan de sécurité de l'information.
- Doit déclarer au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale.
- Doit déclarer au Ministère les risques de sécurité de l'information à portée gouvernementale.

Voir le ***Guide de nomination*** pour plus d'information.

DIRECTIVE DE SÉCURITÉ

Forme abrégée de la **Directive sur la sécurité de l'information à la CSDM**.
La Directive de sécurité est un document officiel de la CSDM concernant les mesures mises en place au sujet de la sécurité de l'information à la CSDM. Ce document décrit les objectifs, le cadre légal et administratif, le champ d'application, les principes directeurs ainsi que les sanctions qui concernent la sécurité de l'information à la CSDM.

DISPONIBILITÉ

Propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

DOCUMENT

Ensemble 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 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 transcrits sous l'une de ces formes ou en un autre système de symboles. Est assimilée 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.

DROIT D'AUTEUR

Droit exclusif de produire ou de reproduire une œuvre ou une partie importante de celle-ci, sous une forme matérielle quelconque, de la représenter en public, de la publier, de permettre l'un des actes ci-dessus énumérés ainsi que tous les droits accessoires y afférents, le tout tel que défini par la Loi sur le droit d'auteur.

FILTRAGE WEB

Activité réalisée par le pare-feu institutionnel, par un serveur ou par un autre dispositif et permettant de bloquer l'accès à certaines ressources d'Internet à partir du réseau interne de la CSDM.

GUIDE DE NOMINATION

Document utilisé avec la ***Directive de sécurité*** ainsi qu'avec le ***Cadre de gestion de la sécurité de l'information et de l'utilisation des technologies*** pour permettre de comprendre les rôles et les compétences requises afin d'identifier et de nommer des responsables pour les rôles de **Coordonnateur sectoriel de la gestion des incidents** (CSGI) et de **Responsable de la sécurité de l'information** (RSI).

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 des systèmes d'information, par exemple en causant une interruption des services ou une réduction de leur qualité.

Incident de sécurité de l'information à portée gouvernementale

La conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale dont les risques d'atteinte à sa disponibilité, à son intégrité ou à sa confidentialité peuvent avoir des conséquences liées à la vie et la santé ou au bien-être des personnes, à l'atteinte à la protection des renseignements personnels et à la vie privée, à la prestation de services à la population ou à l 'image de la CSDM et du gouvernement et nécessitant une intervention concertée au plan gouvernemental.

INFORMATION

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

IMPUTABILITÉ

Principe selon lequel une action/activité peut sans équivoque être attribuée à l'entité qui en est responsable (non-répudiation).

INFRASTRUCTURE TECHNOLOGIQUE

Ensemble des dispositifs mis à la disposition des utilisateurs par la CSDM permettant à des outils technologiques d'accéder à des données ou à des services, notamment :

- Serveurs hébergés à la CSDM
- Serveurs hébergés à l'extérieur de la CSDM et utilisés dans le cadre des activités d'un utilisateur à la CSDM (Infonuagique)
- Équipements de routage et de commutation
- Réseau interne de la CSDM
- Bornes sans fil (wifi)
- Internet

INTÉGRITÉ

Propriété d'une information de ne subir aucune altération ni destruction sans autorisation ou de façon erronée. L'information doit être conservée sur un support et doit être préservée avec des moyens lui procurant stabilité et pérennité.
L'intégrité fait référence à l'exactitude et à la complétude.

INTRANET

Ensemble des éléments de l'infrastructure technologique dont la CSDM est propriétaire et qui sont réservés aux seuls utilisateurs internes, incluant les équipements, les applications et les systèmes qui ne sont disponibles qu'à partir de l'intérieur de la CSDM ou par lien SSL-RPV.

INTERNET

Réseau informatique mondial, également désigné sous l'épithète Web, WWW ou World Wide Web, composé de millions de réseaux aussi bien publics que privés et permettant l'accès à un ensemble d'applications et de services offerts par l'entremise des serveurs qui y sont raccordés.

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.

LIEN SSL-RPV / LIEN RPV / LIEN VPN

Type de connexion cryptée permettant un accès sécurisé à l'intranet à partir d'un outil technologique situé à l'extérieur du réseau interne de la CSDM. L'acronyme SSL réfère au protocole de cryptage des données (*Secure Socket Layer*), alors que l'acronyme RPV, peu utilisé en informatique sous sa forme française, représente l'expression « réseau privé virtuel ». L'acronyme habituellement reconnu pour désigner ce type de connexion est VPN, pour *Virtual Private Network*.

LIGNES DIRECTRICES D'UTILISATION

Forme abrégée des ***Lignes directrices sur l'utilisation des technologies à la CSDM***. Les Lignes directrices d'utilisation est un document officiel de la CSDM concernant les mesures mises en place au sujet de l'utilisation des technologies à la CSDM. Ce document décrit la nature, le champ d'application, les principes directeurs ainsi que les droits, responsabilités et obligations des utilisateurs et des divers intervenants en ce qui concerne l'utilisation des technologies à la CSDM.

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, jeu ou autre).

Logiciel libre

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

Logiciel propriétaire

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.

MESSAGERIE NUMÉRIQUE

Toute forme de système conçu pour la communication entre utilisateurs, notamment les systèmes suivants : courriel, messagerie texte, téléphonie IP, visioconférence ou clavardage.

MESURE DE SÉCURITÉ DE L'INFORMATION

Moyen concret assurant partiellement ou totalement la protection d'information contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs, acte involontaire, acte malveillant tel intrusion, divulgation ou vol de documents, etc.). La mise en œuvre de cette

mesure vise à amoindrir la probabilité d'apparition de ces risques ou à réduire les pertes qui en résultent.

MESURE COMPENSATOIRE

Moyen concret permettant de diminuer la probabilité de matérialisation d'un risque découlant d'une non-conformité à la Directive de sécurité.

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

Outil technologique personnel

Tout outil technologique appartenant en propre à l'utilisateur et permettant un accès à Internet ou à un élément de l'infrastructure technologique de la CSDM.

PARE-FEU INSTITUTIONNEL

Point de démarcation entre l'intranet et Internet, le pare-feu institutionnel protège le caractère privé de l'intranet tout en permettant aux utilisateurs liés au réseau interne de la CSDM d'avoir accès à Internet selon des règles de sécurité.

PLAN DE CONTINUITÉ

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

PLAN DE RELÈVE

Plan de reprise hors site mis en œuvre lorsqu'il y a détérioration ou destruction d'actifs informationnels consécutive à un incident exigeant le transfert de l'exploitation dans un autre lieu. Le plan de relève décrit les procédures visant à assurer, dans des conditions de continuité adaptées aux critères de survie de la CSDM, la mise à la disposition rapide et ordonnée des moyens de secours ainsi que la reprise éventuelle de l'exploitation normale après réfection ou remplacement des actifs détruits ou endommagés.

REGISTRE D'AUTORITÉ

Répertoire, recueil ou fichier dans lequel sont notamment consignées les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information ainsi que les responsabilités qui y sont rattachées.

REGISTRE D'INCIDENT

Recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, le problème à la source, les mesures prises pour le rétablissement à la normale.

RENSEIGNEMENT CONFIDENTIEL

Renseignement ou information 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**. Le consentement du détenteur de l'information doit être obtenu avant de pouvoir divulguer ce renseignement à qui ce soit.

RENSEIGNEMENT PERSONNEL

Information concernant une personne physique et qui permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de la sécurité de l'information.

RÉSEAUX SOCIAUX

Ensemble de personnes réunies virtuellement par un lien social. Sur Internet, un réseau social est un média permettant à un utilisateur de publier des données (vidéos, musique, textes, photographies et autres messages) à l'intention des interlocuteurs de son choix ou publiquement. L'utilisateur peut également voir des données qui lui sont destinées ou pour lesquelles il dispose de droits d'accès. Les réseaux sociaux sur le Web visent à faciliter l'interaction, la collaboration ainsi que le partage et la diffusion de contenus entre utilisateurs.

RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI)

Personne nommée par le Conseil des Commissaires pour occuper un rôle stratégique et relationnel avec la haute direction. Le RSI communique à la CSDM les orientations et les priorités en matière de sécurité de l'information et s'assure de l'arrimage et de la participation de tous les intervenants de la CSDM.

Voir le ***Guide de nomination*** pour plus d'information.

RISQUE DE SÉCURITÉ DE L'INFORMATION

Degré d'exposition d'une information ou d'un système d'information à une menace d'interruption ou de réduction de la qualité des services ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information.

Un risque de sécurité de l'information peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits

fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ou sur l'image de la CSDM.

Risque de sécurité de l'information à portée gouvernementale

Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale. Ce risque peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection de leurs renseignements personnels et au respect de leur vie privée, sur l'image du gouvernement ou sur la prestation de services fournie par d'autres organismes publics.

SECRÉTARIAT GÉNÉRAL

Le Service du secrétariat général s'assure de l'adoption de la **Directive de sécurité** par le Conseil des commissaires et la publie sur le site Web de la CSDM.

SÉCURITÉ DE L'INFORMATION (SI)

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

Le terme sécurité fait autant référence à la cybersécurité qu'à la sécurité de l'information.

SERVEUR

Dispositif informatique qui offre des services à différents clients, par exemple le partage de fichiers, l'accès aux informations sur Internet, le courrier électronique, le partage d'imprimantes, le commerce électronique, le stockage en base de données, le jeu ou la mise à disposition d'applications.

SERVICE DES RESSOURCES HUMAINES*

Service qui s'assure que tout nouvel employé de la CSDM soit avisé de la **Directive de sécurité** et de la **Directive d'utilisation** et obtient du nouvel employé son engagement au respect de ces Directives.

**Note : À la CSDM, le Service de la gestion des personnes et du développement des compétences (SGPDC) correspond au Service des ressources humaines.*

SERVICE DES RESSOURCES MATÉRIELLES (SRM)

Service qui participe, avec le CSGI et le RSI, à l'identification des risques traditionnels et des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels traditionnels de la CSDM.

SERVICE DES TECHNOLOGIES DE L'INFORMATION (STI)

Service qui s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels il intervient:

- Il élabore une stratégie concernant la sécurité de l'information et l'utilisation des technologies à la CSDM.
- Il participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information.
- Il applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, tel que par exemple l'interruption ou la révocation temporaire – lorsque les circonstances l'exigent – des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause.
- Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la Directive de sécurité et autorisées par la direction générale.
- Il met en place une structure permettant l'évaluation régulière de sa stratégie de sécurité et d'utilisation et effectue les corrections nécessaires à son bon fonctionnement.

SYSTÈME D'INFORMATION

Ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

TECHNOLOGIE DE L'INFORMATION

Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

UTILISATEUR OU UTILISATRICE

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 la CSDM détient dans l'accomplissement de sa mission. Les membres du personnel de la CSDM ainsi que les élèves sont les premiers utilisateurs de l'information de la CSDM. Tout utilisateur de ces réseaux doit se conformer aux politiques et aux directives en vigueur dans la CSDM dans le cadre de toutes ses activités lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

Commission scolaire de Montréal

Quiconque utilise un outil technologique fourni par la CSDM ou une composante de l'infrastructure informatique de la CSDM et ayant un lien fonctionnel avec la CSDM, notamment les personnes suivantes :

- Membres du personnel
- Élèves jeunes et adultes
- Parents
- Membres du Conseil des commissaires
- Bénévoles
- Stagiaires
- Consultants
- Employés contractuels
- Sous-traitants
- Organismes externes

Utilisateur interne

Utilisateur disposant d'un code d'identification et d'un mot de passe lui permettant d'utiliser un outil technologique fourni par la CSDM.

Utilisateur externe

Utilisateur ne disposant pas d'un code d'identification fourni par la CSDM.

TÉLÉCHARGEMENT

Opération de transmission d'informations — logiciels, données, images, sons, vidéos ou autres — d'un ordinateur à un autre par l'intermédiaire d'un réseau, en général Internet. Le téléchargement inclut ici la réception d'informations à partir d'un ordinateur distant (téléchargement ou download) de même que le téléchargement vers un ordinateur distant (téléversement ou upload).

TRAÇABILITÉ

Situation où l'on dispose de l'information nécessaire et suffisante pour connaître (éventuellement de façon rétrospective) la composition de l'actif informationnel tout au long de sa chaîne de production, de transformation et de distribution et ce, en quelque endroit que ce soit, depuis son origine première jusqu'à sa fin de vie.