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.