COMMISSION SCOLAIRE DU FER

DIRECTIVE

Cadre de gestion de la sécurité de l'information	SECRÉTARIAT GÉNÉRAL **RÉPONDANT**

ORIGINE	Secrétariat général
DESTINATAIRES :	Directions des unités administratives
Entrée en vigueur : 8 avril 2019	**Résolution no.** : CC-2018-2019 /151

TABLE DES MATIÈRES

PRÉAMBULE 3
OBJECTIFS 4
1. CADRE LÉGAL ET ADMINISTRATIF 5
2. CHAMP D'APPLICATION 5
3. GESTION DES RISQUES ET DES INCIDENTS 5
3.1. Gestion des risques 5
3.2. Gestion des incidents 6
4. DIRECTIVES 6
4.1. Gestion des accès 6
4.2. Privilège 6
4.3. Usage prioritaire 7
4.4. Usage à des fins personnelles 7
4.5. Éthique souhaitée 7
4.6. Comportements interdits 8
4.7. Modification ou destruction 9
4.8. Actes délinquants 9
4.9. Actes illégaux 9
4.10. Accès non autorisé 9
4.11. Utilisation raisonnable 10
4.12. Courrier électronique 10
4.13. Renseignements confidentiels 10
4.14. Obligations de l'usager 11
4.15. Droit d'un usager à la confidentialité 11
4.16. Gestion des vulnérabilités 12
4.17. Vérifications 12
4.18. Intervention 12
4.19. Restauration 12

4.20. Suspension des droits d'accès lors d'une vérification 13
4.21. Sécurité 13
4.22. Collaboration 13
4.23. Gestion des copies de sauvegardes 13
4.24. Continuité des affaires 14
4.25. Protection du périmètre du réseau 14
4.26. Utilisation d'un appareil personnel (B.Y.O.D) 14
4.27. Protection des actifs de l'information format non numérique 14
5. RÔLES ET RESPONSABILITÉS DES COMITÉS ET DES SERVICES 15
5.1. Comité de travail pour la sécurité de l'information 15
5.2. Comité de la gestion des risques et des incidents 15
5.3. Secrétariat général 16
5.4. Service des technologies de l'information 16
5.5. Service des ressources matérielles 16
5.6. Service des ressources humaines 16
5.7. Responsable de l'actif informationnel 17
6. PÉNALITÉS ET SANCTIONS 18
7. SENSIBILISATION ET FORMATION 18
8. DIFFUSION ET MISE À JOUR 19
9. ENTRÉE EN VIGUEUR 19
ANNEXE I – 20
Déclaration d'engagement par les utilisateurs quant au respect des règles de sécurité de l'information 20

PRÉAMBULE

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 commission scolaire) créent des obligations aux établissements scolaires en leur qualité d'organismes publics.

Ainsi, la *Directive sur la sécurité de l'information gouvernementale* oblige la commission scolaire 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.

La Commission scolaire du Fer reconnaît l'importance pour les membres de son personnel et pour les élèves jeunes et adultes fréquentant ses établissements d'avoir accès à ses ressources informatiques et à son réseau de télécommunication. Elle a le devoir de s'assurer que les pratiques d'utilisation des ressources informatiques et du réseau de télécommunication soient conformes à la mission éducative et aux fonctions administratives de la Commission et de ses établissements.

La Commission assume que la conduite de chaque usager est dictée par les règles usuelles de bienséance et de courtoisie ainsi que par le respect des lois et règlements en vigueur. Aussi, la présente politique s'applique à toutes ressources informatiques étant la propriété de la Commission, qu'elles soient situées dans ses établissements ou à l'extérieur de ceux-ci.

En tant que propriétaire et gestionnaire des ressources informatiques et du réseau de télécommunication, la Commission a le devoir de s'assurer que leur utilisation soit conforme à la légalité et s'exerce dans le respect de certaines normes. Ainsi, un contrôle de l'utilisation des actifs informatiques s'avère essentiel. Pour des intérêts sérieux et légitimes, la Commission se réserve le droit d'accéder à ses postes informatiques, de les surveiller au besoin, d'en récupérer, lire ou dévoiler le contenu et d'en retirer le droit d'accès.

Pour ce faire, la commission scolaire *du Fer* s'est dotée d'un cadre de gestion qui permettra aux différents niveaux de gestions de travailler ensemble pour optimiser la mise en place des initiatives de sécurité liées à la politique de la sécurité de l'information.

OBJECTIFS

Le présent cadre de gestion a pour objectif d'identifier les différents comités et leurs responsabilités permettant aux commissions scolaires de s'acquitter pleinement de leurs obligations à l'égard de la sécurité de l'information. Plus précisément :

- le conseil des commissaires;
- le directeur général et le comité consultatif de gestion;
- le comité de travail pour la sécurité de l'information;
- le comité de gestion des risques et des incidents.

Par conséquent, la commission scolaire met en place ce cadre dans le but d'instaurer la synergie entre les différents intervenants qui permettra une mise en œuvre des obligations de la politique de sécurité de l'information.

De plus le présent cadre établit les conditions d'utilisation des ressources numériques et non numériques par les usagers. Il vise à :

- contribuer à la réalisation de la mission éducative;
- promouvoir une utilisation responsable des ressources informatiques;
- préserver la réputation de la commission scolaire comme organisme éducatif responsable;
- prévenir une utilisation abusive ou illégale des ressources numériques et non numériques de la part des usagers;
- assurer la protection des droits d'auteurs;
- assurer la protection des renseignements personnels;
- délimiter les balises de la vie privée des usagers dans leur utilisation des ressources informatiques;
- minimiser les risques de destruction ou de modification des systèmes et des documents.

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 *Politique de sécurité de l'information* adoptée par la commission scolaire.

2. CHAMP D'APPLICATION

Le présent cadre s'adresse aux membres des deux comités mentionnés ci-dessus, c'est-à-dire à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public, siège à un de ces comités.

3. GESTION DES RISQUES ET DES INCIDENTS

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

3.1. Gestion des risques

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 commission scolaire. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*. L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement de la commission scolaire.

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 commission scolaire.

3.2. Gestion des incidents

La commission scolaire 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 commission scolaire peut exercer ses pouvoirs et ses prérogatives en égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

4. DIRECTIVES

Pour chacune des directives élaborées ci-dessous, prévoir une révision à fréquences prédéterminées et procéder à une mise à jour au besoin.

4.1. Gestion des accès

Une gestion des accès logique et physique 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 de conserver ces évidences pour les audits ultérieurs.

4.2. Privilège

L'accès aux ressources informatiques et documents confidentiels de la Commission constitue un privilège et non pas un droit. Seuls les usagers dûment autorisés peuvent y avoir accès et les utiliser, et ce, dans les limites de l'autorisation accordée à l'usager par la Commission. L'usager ne peut permettre qu'un tiers non autorisé utilise ces ressources ni son code d'accès qui peut être révoqué en tout temps par la Commission en raison d'une utilisation inappropriée ou abusive.

L'utilisation de ce privilège doit être raisonnable et ne pas avoir pour effet de limiter indûment l'accès aux ressources aux autres usagers.

4.3. Usage prioritaire

Les ressources informatiques et documents confidentiels sont mis à la disposition des usagers pour la réalisation d'activités d'enseignement, d'apprentissage, de gestion, d'administration et de services à la collectivité reliés à la réalisation de la mission de la Commission et celle de ses établissements, et ce, dans l'exercice des fonctions de chacun des usagers.

Les consultants, les professionnels ou les intervenants externes avec lesquels la Commission transige doivent respecter les pratiques d'utilisation des ressources et du réseau de télécommunication définies dans le présent cadre.

4.4. Usage à des fins personnelles

Les usagers doivent savoir que la Commission peut avoir accès aux communications ou transactions faites au moyen de ses ressources technologiques et que, par conséquent, toute utilisation à des fins personnelles ne peut aucunement être considérée comme privée. Les usagers peuvent utiliser les ressources de la Commission à des fins personnelles à certaines conditions, notamment :

- l'utilisation est faite hors des heures régulières de travail, en autant qu'elle n'entrave pas la performance au travail de l'employé ou celle des autres employés;
- l'utilisation n'entrave pas l'activité pédagogique de l'élève ou celle des autres élèves;
- l'usager respecte les dispositions du présent cadre, et ce, même s'il fait usage des ressources à des fins personnelles;

4.5. Éthique souhaitée

L'usager qui utilise les ressources informatiques et les documents confidentiels de la Commission agit :

- dans le respect des personnes, de leur vie privée, des renseignements personnels ou confidentiels les concernant, et ce, tant dans la communication de messages que d'images;
- dans le respect des droits d'auteurs et de la propriété intellectuelle des autres;
- dans le respect des mesures de sécurité établies par la Commission;
- dans le respect du bien d'autrui mis à sa disposition.

Les comportements interdits énumérés dans ce cadre précisent les gestes qui contreviendraient à l'éthique requise par la Commission dans l'utilisation des ressources.

4.6. Comportements interdits

Toute utilisation des ressources et documents confidentiels de la Commission à des fins non autorisées ou illégales est strictement interdite. Il est interdit notamment :

- de télécharger, de stocker et de diffuser des fichiers contenant des propos ou des images de nature grossière, diffamatoire, offensante, perturbatrice, dénigrante, ou à caractère discriminatoire basé sur la race, la couleur, le sexe, l'orientation sexuelle, l'état civil, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale ou le handicap de quiconque;
- d'utiliser les ressources à des fins de propagande, de harcèlement ou de menace sous quelque forme que ce soit, ou pour jouer un tour à des tiers;
- d'utiliser les ressources pour transmettre de la publicité, faire la promotion ou effectuer des transactions à des fins commerciales personnelles;
- de participer à des jeux d'argent et de paris, de quelque nature que ce soit;
- de participer à des activités de piratage (de musique, jeux, logiciels, etc.) et d'intrusion ou de blocage de systèmes informatiques de quiconque;
- d'utiliser les ressources pour nuire à la réputation de quiconque, de la Commission ou de ses établissements;
- d'associer des propos personnels au nom de la Commission ou à celui d'un établissement dans des groupes de discussions, des séances de clavardage, ou d'utiliser tout autre mode d'échanges d'opinions de manière à laisser croire que les opinions qui y sont exprimées sont endossées par la Commission ou par l'établissement, sauf lorsque cela est fait par une personne autorisée à le faire dans l'exercice de ses fonctions ;
- de clavarder, de participer à des jeux collectifs et d'utiliser une caméra permettant la transmission d'images animées (WEBCAM) avec ou sans la voix sur Internet, sauf si cette participation s'inscrit dans le cadre d'une activité pédagogique ou parascolaire étroitement supervisée et qu'elle se

déroule dans un contexte assurant la sécurité des ressources informatiques, du réseau et des personnes;

- d'utiliser le ou les codes d'accès d'un autre usager ou de prêter son ou ses codes d'accès à un autre usager sauf dans le cadre strict des exigences liées au travail.

4.7. Modification ou destruction

Toute modification ou destruction des ressources est interdite sans l'autorisation de l'autorité compétente. Toute intervention d'ordre physique sur un équipement du réseau de télécommunication est exclusivement réservée au Service des technologies de l'information.

4.8. Actes délinquants

Il est strictement interdit de poser tout acte pouvant nuire au bon fonctionnement des ressources informatiques, entre autres, par l'insertion ou la propagation de virus informatiques, par la destruction ou la modification non autorisée de données, de documents ou de logiciels, ou par des gestes visant à désactiver, défier ou contourner n'importe quel système de sécurité de la Commission.

4.9. Actes illégaux

L'usager est responsable des actes qu'il pose en utilisant les ressources informatiques de la Commission. L'usager qui commet un acte illégal s'expose à une poursuite judiciaire et à une réclamation en dommages.

4.10. Accès non autorisé

À moins d'y être autorisé, il est interdit d'accéder ou de tenter d'accéder à documents, des fichiers, banques de données, systèmes, réseaux internes ou externes dont l'accès est restreint ou limité à une catégorie spécifique d'usagers. Il est également interdit de transmettre, d'utiliser ou de divulguer des données concernant la Commission dans un but autre que celui où l'usager est autorisé à le faire.

4.11. Utilisation raisonnable

Dans un contexte de partage équitable des ressources, l'usager ne doit pas monopoliser ou abuser des ressources numériques et non numériques, par exemple, en s'appropriant un volume, en effectuant un stockage abusif d'information ou en utilisant Internet pour écouter la radio ou une émission de télévision, et ce, en dehors du contexte d'une activité pédagogique ou professionnelle. En tout temps, l'usager doit respecter le droit d'auteur et les autres droits de propriété intellectuelle des tiers.

4.12. Courrier électronique

L'usager doit respecter, lorsqu'il y a lieu, la confidentialité des messages et s'abstenir d'intercepter, de lire, de modifier ou de détruire tout message qui ne lui est pas destiné.

Il est interdit aux usagers :

- d'utiliser un ou des subterfuges ou d'autres moyens pour transmettre un courrier électronique de façon anonyme ou en utilisant le nom d'une autre personne;
- de s'abonner à des listes d'envoi n'ayant aucun rapport avec la fonction de l'usager;
- d'expédier, sans autorisation, à tout le personnel ou à des groupes de membres du personnel, des messages sur des sujets d'intérêt divers, des nouvelles de toutes sortes, des lettres en chaîne et toute information non pertinente aux activités de la Commission ou de ses établissements qui auraient pour effet d'accaparer la bande passante du réseau de télécommunication.

4.13. Renseignements confidentiels

L'information contenue dans les ressources numériques et non numériques est confidentielle lorsqu'elle a le caractère d'un renseignement personnel ou d'un renseignement que la Commission protège en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, ou le caractère d'un renseignement relatif à la vie privée de la personne au sens du *Code civil du Québec.*

4.14. Obligations de l'usager

Respect des mécanismes de protection : l'usager doit respecter les règles édictées par la Commission quant à la conservation, l'accès, la transmission et la diffusion des renseignements personnels.

Diffusion de renseignements personnels : l'usager ne peut diffuser, sans le consentement des personnes concernées, des renseignements personnels sous forme de **renseignements** écrits, de photographies ou d'autres documents visuels montrant les personnes dans des activités permettant de les identifier de façon nominative.

L'usager, lorsqu'il est un élève, doit être informé des comportements à adopter dans la **transmission** de renseignements personnels le concernant ou concernant des membres de sa famille, des amis ou toute autre personne.

4.15. Droit d'un usager à la confidentialité

La Commission respecte la vie privée des usagers. Toutefois, du fait que les ressources numériques et non numériques sont mises à la disposition des usagers pour contribuer à la réalisation de la mission de la Commission et celle de ses établissements, le droit à la vie privée de l'usager est limité. Ainsi, les équipements, documents et fichiers de travail doivent être accessibles en tout temps par la direction, tout employé suppléant ou l'administrateur du réseau.

La Commission ne contrôlera pas systématiquement les communications des usagers. Un contrôle aura lieu seulement s'il y a raison de croire que les systèmes sont utilisés de façon non convenable ou s'il est nécessaire de le faire dans le but de retracer une information qui ne serait autrement disponible.

L'usager perd son droit à la confidentialité des fichiers qu'il a créés lorsqu'il utilise les ressources ou toute information contenue en contravention à la présente politique ou à des directives et règles émises par la Commission pour en assurer l'application ou à des ententes ou protocoles pertinents de la Commission, ou aux lois ou règlements provinciaux ou fédéraux.

L'usager doit savoir que la Commission peut être appelée, dans le cadre d'une procédure judiciaire, à produire en preuve le contenu de tout document qu'elle détient. Dans un tel cas, la Commission se réserve le droit et la possibilité, sans préavis, d'inspecter et contrôler toutes les données.

4.16. Gestion des vulnérabilités

La commission scolaire déploie des mesures pour maintenir à jour son parc informatique afin de maintenir les vulnérabilités des actifs de l'information 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.

4.17. Vérifications

La Commission se réserve le droit de tenir un registre des transactions effectuées avec ses ressources informatiques et son réseau de télécommunication et celui d'analyser les informations contenues dans ce registre afin de détecter les activités non autorisées, illicites ou illégales sur son réseau.

Les directions d'établissement et de service sont autorisées en tout temps et sans préavis à procéder à toutes les vérifications estimées nécessaires et à effectuer et conserver toutes copies de documents, données ou information pour s'assurer du respect des dispositions de la politique et des directives et règles émises par la Commission pour assurer l'application des ententes et protocoles pertinents de la Commission ou des lois ou des règlements provinciaux ou fédéraux.

Le Service des technologies de l'information peut procéder à toute vérification sans préavis lorsqu'une situation d'urgence le justifie, par exemple, la détection de la présence d'un virus dans le réseau ou une utilisation excessive des ressources du réseau.

4.18. Intervention

La Commission se réserve le droit d'enlever de ses ressources informatiques tout contenu illégal ou qui contrevient aux dispositions du présent cadre.

4.19. Restauration

Le matériel informatique de la Commission peut être réinitialisé à son état original s'il a été endommagé ou affecté par tout acte contrevenant à la politique.

4.20. Suspension des droits d'accès lors d'une vérification

Les droits d'accès d'un usager peuvent être suspendus pendant la durée d'une vérification. Une telle décision incombe au supérieur immédiat ou à la direction des ressources humaines lorsqu'il s'agit d'un employé ou au directeur de l'établissement lorsqu'il s'agit d'un élève ou d'un parent.

4.21. Sécurité

Le Service des technologies de l'information met en place les outils informatiques assurant :

- la sécurité des ressources informatiques;
- la protection contre les virus, les intrusions ou les altérations de données;
- la prévention des utilisations illicites.

Le Service des technologies de l'information peut édicter des directives et règles pour assurer la sécurité des ressources informatiques, et procéder périodiquement à des audits de sécurité.

4.22. Collaboration

L'usager collabore avec le Service des technologies de l'information afin de faciliter l'identification et la correction des problèmes ou anomalies pouvant se présenter concernant les équipements et les ressources informatiques de la Commission en les signalant à la personne responsable de son établissement.

4.23. Gestion des copies de sauvegardes

La commission scolaire 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.

4.24. Continuité des affaires

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

4.25. Protection du périmètre du réseau

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

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

L'utilisation d'un appareil personnel (iPad, téléphone intelligent, etc.) par un employé **dans l'exercice de ses fonctions** doit respecter la politique et le cadre de la commission scolaire afin de protéger les données de celle-ci. Pour les élèves, les parents ou les partenaires, les mêmes règles d'utilisation s'appliquent.

4.27. Protection des actifs de l'information format non numérique

La commission scolaire doit se doter et appliquer une directive de protection des actifs de l'information non numérique qui sont en lien principalement aux classeurs et imprimantes. 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 doit être considérée dans l'élaboration de cette directive. Cette protection inclut la gestion des accès physiques aux salles, aux imprimantes ou autres endroits qui détiennent des actifs de l'information non numérique. Cette directive de la protection du périmètre prévoit faire des audits et ainsi de les protéger lors du transit d'un endroit à un autre. Ce mandat pourrait être confié au comité de gestion des risques et des incidents.

5. RÔLES ET RESPONSABILITÉS DES COMITÉS ET DES SERVICES

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

5.1. Comité de travail pour la sécurité de l'information

Le comité de travail pour 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 autre élément pouvant être nécessaire pour assurer la protection de la commission scolaire et être conforme à la réglementation. C'est un comité qui est tactique et opérationnel.

Ce comité est chargé de mettre en place 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 sera formé des parties prenantes de la commission scolaire qui seront directement concernées ou qui participent à la mise en œuvre de la sécurité de l'information.

5.2. Comité de la gestion des risques et des incidents

Le comité de la gestion des risques et des incidents a la responsabilité de monter une équipe de réponses aux incidents de sécurité numériques et non numériques et d'établir une procédure de réponses aux incidents. Ce comité doit comprendre le CSGI, RSI, DG, SG, directeurs de services ainsi que tous employés jugés essentiels. Le comité doit s'assurer que les contrôles sont en place pour identifier un incident lorsqu'il se produit ou s'est produit. Le comité doit s'assurer que des tests aux réponses d'incidents doivent être conduits périodiquement pour vérifier son efficacité. De plus, il doit faire l'analyse de ces processus d'affaires et identifier ceux qui auront un impact majeur à la commission scolaire s'ils venaient à ne plus être fonctionnels et que la prestation de services était arrêtée.

5.3. Secrétariat général

La direction du Secrétariat général valide les politiques en sécurité informationnelle (SI).

5.4. Service des technologies de l'information

En matière de sécurité de l'information, le Service des technologies de l'information 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 des systèmes d'information dans lesquels il intervient :

- 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 numériques 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 entraves à la présente politique et autorisées par le directeur général.

5.5. Service des ressources matérielles

Le Service des ressources matérielles participe, avec le CSGI/RSI à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels de la commission scolaire.

5.6. Service des ressources humaines

En matière de sécurité de l'information, le Service des ressources humaines s'assure que tout nouvel employé de la commission scolaire soit avisé de la politique de sécurité de l'information et obtient son engagement au respect de la politique.

5.7. Responsable de l'actif informationnel

Le responsable de l'actif informationnel est le cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif (Service des ressources financières, Service des ressources éducatives, directions d'établissements, etc.), et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité ces actifs 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.

- Il informe le personnel relevant de son autorité de la politique 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;
- Il collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques;
- Il voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la politique de sécurité de l'information et de tout autre élément du cadre de gestion;
- Il s'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion;
- Il rapporte au CSGI toute menace, incident ou problème afférant à la sécurité de l'information ou à l'application de la politique;
- Il collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'actif de l'information numérique et non numérique.

6. PÉNALITÉS ET SANCTIONS

L'usager qui contrevient aux dispositions de ce cadre ou de la politique émises par la Commission pour en assurer l'application, peut faire l'objet des pénalités et des sanctions prévues par les lois et règlements pertinents, des mesures disciplinaires prévues dans les règlements et les conventions collectives régissant le personnel et celles prévues par un établissement dans ses règles de conduite et de comportement régissant les élèves. Ces mesures peuvent aller jusqu'au congédiement ou à l'expulsion.

De plus, l'une ou plusieurs des sanctions administratives suivantes pourront être appliquées**:**

- l'annulation du code d'accès et des mots de passe de l'usager;
- l'interdiction d'utiliser en totalité ou en partie les ressources numériques et non numériques;
- la destruction sans préavis des documents constitués contrairement au présent cadre, illégalement ou comportant des informations à caractère illicite;
- l'obligation de rembourser à la Commission toute somme que celle-ci serait appelée à défrayer à titre de dommages, de pénalités ou autres à la suite de la contravention.

Le supérieur immédiat d'un employé ou l'administrateur du Service des technologies de l'information ou le directeur du Service des ressources humaines est responsable de voir à l'imposition des sanctions prévues aux alinéas précédents selon les circonstances lorsque l'usager est un membre du personnel. Le directeur de l'établissement est responsable de voir à l'imposition des sanctions lorsque l'usager est un élève ou un parent.

7. SENSIBILISATION ET FORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté de la commission scolaire doivent être formés et sensibilisés :

- à la sécurité de l'information et des systèmes d'information de la commission scolaire;
- aux directives de la sécurité;
- à la gestion des risques;

- à la gestion des incidents;
- aux menaces existantes;
- aux conséquences d'une atteinte à la sécurité;
- à leur rôle et à leurs responsabilités en la matière.

Des documents explicatifs sont disponibles sur le site Internet de la commission scolaire.

8. DIFFUSION ET MISE À JOUR

Le comité de travail pour la sécurité de l'information (RSI et CSGI) s'assure de la diffusion et de la mise à jour du cadre. Celui-ci sera révisé périodiquement selon les mises à jour effectuées.

De plus, les directions d'établissements et de services sont responsables de l'application de la politique ainsi que du cadre au sein de leur établissement ou de leur service.

9. ENTRÉE EN VIGUEUR

Le présent cadre est en vigueur depuis le *8 avril 2019.*

ANNEXE I – Déclaration d'engagement par les utilisateurs quant au respect des règles de sécurité de l'information

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par la commission scolaire. À cette fin, ils doivent :

- ✓ Se conformer aux directives de la commission scolaire, à la politique sur la sécurité de l'information ainsi qu'aux directives sectorielles, aux procédures et aux autres lignes de conduite se rapportant à la sécurité de l'information de la commission scolaire;
- ✓ 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;
- ✓ 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 commission scolaire;
- ✓ Au moment de leur départ de la commission scolaire, remettre les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de l'exercice de leurs fonctions.

Je, soussigné(e), _____, reconnais avoir pris connaissance des règles, ci-dessus reproduites, sur la sécurité de l'information de la commission scolaire et m'engage à les respecter.

Signature : _____

Date : _____