- ○ Règlement
- ○ Politique
- ◉ Pratique de gestion

Approbation : Direction générale
Résolution : Sans objet
Responsable : Responsable de la sécurité de l'information (RSI)
Date d'approbation : 4 décembre 2018
Date d'entrée en vigueur : 4 décembre 2018
Date prévue de révision : Au besoin
Date d'annulation :
Date de l'avis public préalable : Sans objet
Date de l'avis public d'adoption : Sans objet

Liste des écrits de gestion remplacés :

Consultations effectuées :
CCG du 15 novembre 2018.

Date des amendements : Sans objet

Ce document a été rédigé en respectant les règles de la nouvelle orthographe de l'Office de la langue française.

TABLE DES MATIÈRES

1. PRÉAMBULE ... 3

2. OBJECTIFS ... 3

3. CADRE LÉGAL ET ADMINISTRATIF ... 3

4. CHAMP D'APPLICATION ... 3

5. GESTION DES RISQUES ... 3

6. GESTION DES INCIDENTS ... 4

7. DIRECTIVES ... 4
Gestion des accès ... 4
Gestion des vulnérabilités ... 5
Gestion des copies de sauvegardes ... 5
Continuité des affaires ... 5
Protection du périmètre du réseau ... 5
Utilisation d'un appareil personnel (B.Y.O.D) ... 5
Protection des actifs de l'information format non numérique ... 5
Gestion des fournisseurs ... 6
L'Internet des objets (IDO) *en anglais IOT* ... 6

8. CADRE DE GESTION ... 6
Conseil des commissaires ... 6
Direction générale et son comité de direction ... 6
Comité de travail pour la sécurité de l'information ... 6
Comité de la gestion des incidents et de la continuité des affaires ... 7

9. RÔLES ET RESPONSABILITÉS ... 7
Direction générale ... 7
Responsable de la sécurité de l'information (RSI) ... 7
Coordonnateur sectoriel de la gestion des incidents (CSGI) ... 9
Secrétaires généraux ... 10
Service des technologies de l'information ... 10
Service des ressources matérielles ... 10
Service des ressources humaines ... 10
Détenteur de l'information ... 10
Utilisateurs ... 11

10. SENSIBILISATION ET FORMATION ... 11

11. DIFFUSION ET MISE À JOUR ... 11

12. ENTRÉE EN VIGUEUR ... 11

ANNEXE 1 – Déclaration d'engagement par les utilisateurs quant au respect des règles de sécurité de l'information ... 12

1. 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. Pour ce faire, la Commission scolaire Pierre-Neveu 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.

2. 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;
- La direction générale et son comité de direction;
- Le comité de travail pour la sécurité de l'information;
- Le comité de gestion d'incidents et de continuité des affaires.

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.

3. 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.

4. CHAMP D'APPLICATION

Le présent cadre s'adresse aux membres des 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.

5. GESTION DES RISQUES

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaitre 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 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.

6. 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 ayant une portée gouvernementale sont déclarés au ministère de l'Éducation et de l'Enseignement supérieur (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.

7. DIRECTIVES

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

<u>Gestion des accès</u>

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.

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.

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.

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.

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 devrait être mis en place pour augmenter le niveau de protection. Aussi, segmenter son réseau permet à la commission scolaire de diminuer les chances de propagation d'un virus ou d'une attaque.

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

Une directive 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 commission scolaire doivent être protégées.

Une entente doit être signée entre les parties énumérant leurs responsabilités respectives.

Protection des actifs de l'information format non numérique

La Commission scolaire doit se doter d'une directive de protection des actifs de l'information non numérique qui sont liés 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 tests d'intrusions ainsi que les protéger lors du transit d'un endroit à un autre.

Gestion des fournisseurs

La Commission scolaire 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, une entente doit être signée avec le fournisseur qui stipule qu'il s'engage à répondre aux exigences en cybersécurité de la commission scolaire et que la commission scolaire 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 services attendus par ce fournisseur. Les fournisseurs ont accès à l'information sensible de la commission scolaire, c'est pourquoi une entente de confidentialité doit être signée avec le fournisseur dans le but de diminuer le risque d'une divulgation de cette information.

L'Internet des objets (IDO) *en anglais IOT*

La Commission scolaire 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.

8. CADRE DE GESTION

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.

Conseil des commissaires

Le conseil des commissaires approuve la nomination des responsables en sécurité de l'information nommés dans la commission scolaire et adopte la *Politique de sécurité de l'information* ainsi que toute modification à celle-ci. Selon les étapes menant à l'adoption d'une politique au sein d'une commission scolaire, le conseil est régulièrement informé des actions d'une commission scolaire en matière de sécurité de l'information.

Direction générale et son comité de direction

La direction générale de la commission scolaire, étant la première 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 commission scolaire en matière de sécurité de l'information. Ainsi, avec les membres de son comité de direction, 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 de la politique.

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 règlementation. 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.

Comité de la gestion des incidents et de la continuité des affaires

Le comité de la gestion des incidents et de la continuité des affaires 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 et SG. 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.

Le comité 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. Ce comité doit prévoir réaliser des tests de continuités des affaires pour en valider l'efficacité.

9. RÔLES ET RESPONSABILITÉS

Direction générale

Tel que prescrit par la *Directive sur la sécurité de l'information gouvernementale* (DSIG), la direction générale d'une commission scolaire est la première responsable de l'information relevant de son autorité. Celle-ci sera soutenue par le projet SICS dans l'atteinte de ses objectifs. Plus précisément, elle a la responsabilité de :

- Désigner ses principaux intervenants en sécurité de l'information à la condition que le conseil des commissaires lui ait délégué cette tâche.
- Mettre en œuvre une politique et un cadre de gestion de la sécurité de l'information au sein de son organisation.
- Définir et mettre en place, de façon formelle, les processus majeurs de sécurité de l'information. Ces processus porteront principalement sur la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents de sécurité de l'information.
- Présenter au Ministère, tous les deux ans, un plan d'action et un bilan de sécurité de l'information, conformément aux modalités et aux formats fixés par ce dernier.
- Déclarer au COGI-réseau les incidents de sécurité de l'information à portée gouvernementale lorsque ceux-ci se produisent.
- Déclarer annuellement au Ministère les risques de sécurité de l'information à portée gouvernementale.
- Appuyer les initiatives et les activités des principaux intervenants désignés en SI (RSI et CSGI).

Responsable de la sécurité de l'information (RSI)

Le rôle et les responsabilités présentés ci-dessous pour le RSI sont semblables à ceux du ROSI-réseau (MEES), soit :

1) Conseil, arrimage et communication :

- Conseiller la haute direction de la commission scolaire en ce qui a trait à la détermination des orientations stratégiques et priorités d'intervention de sa commission scolaire en SI.
- Assurer l'arrimage de toutes les préoccupations en matière de SI de sa commission scolaire incluant celles associées aux technologies de l'information et aux médias papier (ex. : s'assurer que la mise en œuvre des livrables ne viendra pas influencer la capacité de livraison des services de la CS).
- Communiquer à sa commission scolaire, à la demande de la direction générale, les orientations et les priorités d'intervention gouvernementales en matière de SI et celles émanant du DRI du MEES.
- S'assurer de la participation de sa commission scolaire à la mise en œuvre des processus officiels de la gestion de la SI.
- Assurer la coordination et la cohérence des actions de la SI menées au sein de sa commission scolaire par d'autres acteurs, tels que les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique.
- Établir des liens avec les autres RSI de son réseau afin de privilégier le partage d'expertises et d'éléments stratégiques et tactiques à élaborer et à mettre en œuvre (ex. : veille, catégorisation des actifs de l'information, leçons apprises, élaboration et mise en œuvre des processus de gestion SI).

2) Mise en œuvre :

- Coordonner la mise en œuvre des processus officiels de la SI au sein de sa commission scolaire en fonction des livrables élaborés par le Projet de la sécurité de l'information dans les commissions scolaires (SICS).
- Mettre en place et animer les comités internes de coordination et de concertation en sécurité de l'information au sein de sa commission scolaire (ex. : table de concertation pour la catégorisation de l'information incluant les détenteurs de l'information, un représentant des TI, etc.).
- Coordonner l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information en fonction de l'approche préconisée par le projet SICS (ex. : capsules d'information ou vidéos, webinaires par sujet, sessions d'information, etc.).
- Mettre en œuvre, en collaboration avec les autres RSI et le MEES, un processus de veille sur les menaces et les vulnérabilités et sur les bonnes pratiques de sécurité de l'information (ex. : abonnements aux notifications de fournisseurs spécialisés en vulnérabilité et aux magazines portant sur la SI, balayages, participation à des conférences, etc.).

3) Reddition de comptes :

- Soumettre de façon biennale à la direction générale de sa commission scolaire la politique, 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 SI de sa commission scolaire.
- Soumettre annuellement à la direction générale de sa commission scolaire, la déclaration des risques à portée gouvernementale (RPG).

Coordonnateur sectoriel de la gestion des incidents (CSGI)

Collaborant étroitement avec le COGI-réseau du MEES, le CSGI d'une commission scolaire 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 son organisation auprès du CERT/AQ. Pour remplir son rôle, il a comme responsabilités :

1) Mise en œuvre :

- Contribuer à la mise en œuvre des processus officiels de la SI au sein de sa commission scolaire en fonction des livrables définis par le Projet de la sécurité de l'information dans les commissions scolaires (SICS), tels :

  - Une politique en SI.
  - Un cadre de gestion.
  - Un registre d'autorité.
  - La catégorisation des actifs.
  - Des mesures de sécurité pour les actifs critiques.
  - Un processus formel de gestion des risques en SI.
  - Un processus formel de gestion et de déclaration des incidents.
  - Un processus formel de gestion des droits d'accès à l'information.
  - Un processus formel de gestion des vulnérabilités de sécurité (correctifs).
  - Un processus formel de gestion des sauvegardes.

2) Tâches récurrentes :

- Établir des liens avec les autres CSGI afin de privilégier le partage d'expertises et des éléments tactiques et opérationnels à élaborer et à mettre en œuvre.
- Coordonner la gestion des incidents à portée gouvernementale.
- Mettre en place, si elle n'est pas existante, une équipe de réponse aux incidents (ERI) dans sa commission scolaire.
- Avec les membres de l'ERI, développer, mettre en place et tester un plan de réponse aux incidents de sécurité de leur commission scolaire.
- Participer avec le COGI-réseau au processus gouvernemental de gestion des incidents, et au réseau d'alerte gouvernemental coordonné par le CERT/AQ. (aviser le CERT/AQ de tout incident à : incidents-SI@education.gouv.qc.ca).
- Contribuer aux analyses des risques de la SI, de définir les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées pour sa commission scolaire (ex. : exposition aux cyberattaques).
- Contribuer à l'autoévaluation de la sécurité des systèmes informatiques et des réseaux informatiques de sa commission scolaire, notamment par des exercices d'audit de sécurité et des tests d'intrusion aux systèmes jugés à risques.
- Tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications mis en place dans sa commission scolaire.
- Maintenir une veille continue sur les risques, les menaces et les vulnérabilités, par exemple en assistant hebdomadairement aux téléconférences du CERT/AQ, en s'abonnant aux notifications de fournisseurs spécialisés en vulnérabilité et aux magazines portant sur la SI, en effectuant des balayages, en participant à des conférences, etc.).

Secrétaires généraux

Les secrétaires généraux valident les politiques en SI. Ils préparent les résolutions pour les nominations et les politiques et s'assurent de la conformité au cadre législatif.

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, 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 présente politique et autorisées par la direction générale.

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.

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.

Détenteur de l'information

Le détenteur de l'information est le 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 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 et les tiers avec lesquels transige le service 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;
- Collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques;
- 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;

- 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;
- Rapporte au CSGI toute menace ou tout incident afférant à la sécurité de l'information;
- 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;
- Rapporte au CSGI tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de cette politique.

Utilisateurs

Tout utilisateur de la commission scolaire doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

10. 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.

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 commission scolaire.

11. DIFFUSION ET MISE À JOUR

Le RSI, assisté de la direction générale, 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.

12. ENTRÉE EN VIGUEUR

Le présent cadre est entré en vigueur à la date de son approbation par la direction générale.

ANNEXE 1 – 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;
- ✓ S'engager à assurer la sécurité de son appareil mobile personnel si celui-ci sert à un usage professionnel (exemple : mot de passe sécuritaire);
- ✓ 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 différentes cartes d'identité et d'accès, 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 : _____