COMMISSION SCOLAIRE
du Pays-des-Bleuets

N/Réf. : 123-01

CADRE DE GESTION
DE LA SÉCURITÉ DE L'INFORMATION

SERVICE DISPENSATEUR :	Service du secrétariat général et Service des ressources informatiques
PREMIÈRE ADOPTION : (nº résolution)	Le 27 février 2018 (CC-8003-02-18)
MODIFICATIONS : (nos résolutions)	

1.0 CONTEXTE

La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) (RLRQ, chap. G-1.03) et la Directive sur la sécurité de l'information gouvernementale (DSIG), directive du Secrétariat du Conseil du trésor, applicables à la Commission scolaire du Pays-des-Bleuets, créent des obligations aux établissements scolaires en leur qualité d'organismes publics.

Ainsi, la DSIG oblige la Commission scolaire à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'un cadre de gestion de la sécurité de l'information – dont les principales modalités sont définies dans la directive – 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. Tel qu'il est stipulé dans le Guide de nomination, un responsable de la sécurité de l'information (RSI) et un coordonnateur sectoriel de la gestion des incidents (CSGI) doivent être désignés.

2.0 OBJECTIF

Le présent cadre de gestion a pour objectif d'identifier les différents comités et leurs responsabilités permettant à la Commission scolaire de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information.

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

3.0 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 la sécurité de l'information adoptée par la Commission scolaire.

4.0 CHAMPS D'APPLICATION

Le présent cadre de gestion s'adresse à toute personne physique ou morale, à titre d'employé, de consultant, de partenaire, de fournisseur, d'élève ou de public.

5.0 RÔLES ET RESPONSABILITÉS

5.1 Direction générale

Tel que prescrit par la 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 de la sécurité de l'information dans les commissions scolaires (SICS) dans l'atteinte de ses objectifs. Plus précisément, elle a la responsabilité de :

- Désigner les principaux intervenants en sécurité de l'information;
- 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 de l'Éducation et de l'Enseignement supérieur (MEES), 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 coordonnateur organisationnel de gestion des incidents des réseaux (COGI-réseau) du MEES les incidents de sécurité de l'information à portée gouvernementale lorsque ceux-ci se produisent;
- Déclarer annuellement au MEES les risques de sécurité de l'information à portée gouvernementale;
- Appuyer les initiatives et les activités des principaux intervenants désignés en sécurité de l'information (SI).

Pour la soutenir dans l'exercice de ses fonctions, il est impératif qu'elle se dote d'un personnel qualifié sur les plans stratégiques, tactiques et opérationnels ou qu'elle partage, avec d'autres établissements de son réseau, des expertises déjà en place. Ces ressources porteront les noms de « responsable de la sécurité de l'information » (RSI) et « coordonnateur sectoriel de la gestion des incidents » (CSGI).

5.2 Responsable de la sécurité de l'information (RSI)

Le rôle et les responsabilités présentés ci-dessous pour le RSI sont semblables à ceux du responsable organisationnel de la sécurité de l'information (ROSI-réseau) du MEES, soit :

5.2.1 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 papiers (ex. : s'assurer que la mise en œuvre des livrables ne viendra pas impacter la capacité de livraison des services de la Commission scolaire);
- 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 dirigeant réseau de l'information (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).

5.2.2 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 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.).

5.2.3 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 événement 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).

5.3 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 (équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise).

Pour remplir son rôle, il a comme responsabilités :

5.3.1 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 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.

5.3.2 Tâches récurrentes

- Établir des liens avec les autres CSGI afin de privilégier le partage d'expertises et d'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 la 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.
- Contribuer aux analyses des risques de la SI, définir les menaces et les situations de vulnérabilité et 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.

5.4 Secrétaire général

Le secrétaire général valide et approuve les politiques en SI. Il prépare les résolutions pour les nominations et les politiques et s'assure de la conformité au cadre législatif.

5.5 Services des ressources informatiques

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

- Il participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information;
- Il applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, tel que par exemple l'interruption ou la révocation temporaire – lorsque les circonstances l'exigent – des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause;
- Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes au présent cadre de gestion et à la Politique de la sécurité de l'information autorisées par la direction générale.

5.6 Service des ressources matérielles

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

5.7 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 est avisé de la

Politique de la sécurité de l'information et qu'il a signé son engagement au respect de la politique.

5.8 Détenteur de l'information

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

- Informe le personnel relevant de son autorité et les tiers avec lesquels transige son service ou son établissement de la Politique de la sécurité de l'information et des dispositions du cadre de gestion dans le but de les sensibiliser à la nécessité de s'y conformer;
- Collabore activement à la catégorisation de l'information du service ou de l'établissement 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 la 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 Service des ressources informatiques toute menace ou tout incident afférents 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'information;
- Rapporte à la direction générale tout problème lié à l'application de la Politique de la sécurité de l'information et du présent cadre de gestion, dont toute contravention réelle ou apparente d'un membre du personnel, d'un consultant, d'un partenaire, d'un fournisseur, d'un élève ou du public.

5.9 Utilisateurs

Tout utilisateur doit se conformer aux politiques et aux directives en vigueur à la Commission scolaire avec lesquelles il est en relation dans le cadre de ses activités professionnelles ou de scolarisation lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

6.0 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 que des besoins de la Commission scolaire en matière de réduction du risque associé à la protection de l'information.

6.1 Conseil des commissaires

Le conseil des commissaires nomme des responsables en sécurité de l'information pour la Commission scolaire et adopte la Politique de la sécurité de l'information ainsi que le cadre de gestion. Le conseil est régulièrement informé des actions de la Commission scolaire en matière de sécurité de l'information.

6.2 Direction générale et table des directions de service

La direction générale, étant la première responsable de la sécurité de l'information au sein de la Commission scolaire, détermine des mesures visant à favoriser l'application de la Politique de la sécurité de l'information, du présent cadre de gestion et des obligations légales de la Commission scolaire en matière de sécurité de l'information. Ainsi, avec les membres de la table des directions de service, 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. Elle informe le conseil des commissaires des actions posées en matière de sécurité de l'information.

6.3 Comité de travail pour la sécurité de l'information (nouveau)

Le comité de travail pour la sécurité de l'information a comme objectif d'assister le RSI à mettre en place des actions pouvant être nécessaires 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 au projet de mise en place de la sécurité de l'information.

La composition de ce comité est déterminée comme suit :

- RSI;
- CSGI;
- CSGI (substitut);

- Un responsable du Service des ressources informatiques;
- Techniciens affectés à la sécurité.

Au besoin, des intervenants de divers services peuvent en faire partie à titre d'invités.

Les rencontres auront lieu deux fois par année (octobre et mai).

7.0 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. Ce dernier sera révisé périodiquement selon les mises à jour effectuées.

8.0 ENTRÉE EN VIGUEUR

Le présent cadre de gestion entre en vigueur le jour suivant son adoption par le conseil des commissaires.

Dans le présent cadre de gestion, là où la forme masculine est utilisée, c'est sans aucune discrimination et uniquement dans le but d'alléger le texte.