Commission scolaire de la Baie-James

Politique relative à la sécurité de l'information

ADOPTÉE LE : 30 avril 2019 **RÉSOLUTION :** CC3899-19

TABLE DES MATIÈRES

1. CONTEXTE

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) (LRQ, Chapitre G-1.03) 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 DSIG oblige la Commission scolaire à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique relative à la 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. Tel qu'il est stipulé dans le Guide de nomination, un responsable de la sécurité de l'information (RSI) et deux (2) coordonnateurs sectoriels de la gestion des incidents (CSGI) doivent être désignés.

Cette politique permet à la Commission scolaire de la Baie-James de respecter ses obligations, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue. Cette information liée aux ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et papiers, dont les risques d'atteinte à sa disponibilité, son intégrité ou sa confidentialité peuvent avoir des conséquences liées à :

- La vie, la santé ou le bien-être des personnes;
- L'atteinte à la protection des renseignements personnels et à la vie privée;
- La prestation de services à la population;
- L'image de la commission scolaire et du gouvernement.

2. OBJECTIFS

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

Plus précisément, la Commission scolaire doit veiller à :

- La **disponibilité** de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- L'**intégrité** de l'information de manière à ce qu'elle ne soit ni détruite, ni altérée d'aucune façon sans autorisation et que, le support de cette information lui procure la stabilité et la pérennité voulues;
- La **confidentialité** de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

La Commission scolaire, par la mise en place de cette politique, oriente et de détermine sa vision. Une instruction sur la sécurité de l'information en précisera les modalités d'application.

3. CADRE LÉGAL ET ADMINISTRATIF

La politique relative à la sécurité de l'information s'inscrit principalement dans un contexte régi par :

- La Charte des droits et libertés de la personne (LRQ, chapitre C-12);
- La Loi sur l'instruction publique (L.R.Q. c. I-13.3);
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (L.R.Q. c. A-21.1, r.1);
- Le Code civil du Québec (LQ, 1991, chapitre 64);
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, Loi 133);
- La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- Le Code criminel (LRC, 1985, chapitre C-46);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2);
- La Directive sur la sécurité de l'information gouvernementale;

- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- La politique sur la gestion des dossiers personnels de l'élève;
- La politique sur les droits d'auteur;
- La politique sur l'utilisation de la vidéosurveillance avec enregistrement;
- La politique sur l'utilisation des ressources informatiques et du réseau de communication incluant les téléphones intelligents et les médias sociaux.

4. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à toute personne physique ou morale qui, à titre de membre du personnel (commissaire, gestionnaire et employé toutes catégories confondues), de consultant, de partenaire (intervenant de la santé, parent ou autre), de fournisseur, d'élève, de stagiaire ou personne du public, utilise les actifs informationnels de la Commission scolaire.

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

5. PRINCIPES DIRECTEURS

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

- S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité;
- Reconnaître l'importance de la politique de la sécurité de l'information;
- Reconnaître que l'environnement technologique est en changement constant et interconnecté avec le monde;
- Protéger l'information tout au long de son cycle de vie (création, traitement, destruction);
- S'assurer que chaque employé ait accès au minimum d'information requis pour accomplir ses tâches normales;
- Encadrer l'utilisation des actifs de l'information numérique et papier par les utilisateurs.

6. 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 papier 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 elle est exposée;
- Des conséquences de la matérialisation de ces risques;
- Du niveau de risque acceptable par la Commission scolaire.

7. 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'elle détient ou de ses systèmes d'information.

8. DIRECTIVES

8.1 Gestion des accès

Une gestion des accès doit être élaborée, encadrée et contrôlée pour faire en sorte de protéger la disponibilité, l'intégrité et la confidentialité de l'information. Cette gestion doit inclure l'approbation, la revalidation et la destruction de ces accès et de conserver ces évidences pour les audits ultérieurs. Chaque direction d'unité administrative est responsable de l'application de cette mesure.

8.2 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 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. Le RSI et les CSGI sont responsables de l'application de cette mesure.

8.3 Gestion des copies de sauvegardes

La Commission scolaire doit élaborer une stratégie de copie de sauvegarde pour se prémunir contre une perte de données. 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. Le RSI et les CSGI sont responsables de l'application de cette mesure.

8.4 Continuité des affaires

La Commission scolaire doit élaborer une stratégie de continuité des affaires advenant qu'un incident causerait l'arrêt de la prestation de service de cette dernière. Cette stratégie doit être testée à une fréquence adéquate et les écarts corrigés. Le Service des ressources informatiques est responsable de l'application de cette mesure.

8.5 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, en segmentant son réseau, la Commission scolaire limite les chances de propagation d'un virus ou d'une attaque. Le Service des ressources informatiques est responsable de l'application de cette mesure.

8.6 Utilisation d'un appareil personnel (B.Y.O.D) [1]

Une directive sur l'utilisation d'un appareil personnel (iPad, téléphone intelligent, ordinateur portable, etc.) dans l'exercice des fonctions professionnelles sera élaborée pour bien encadrer cette pratique. Les données de la Commission scolaire doivent être protégées.

Une entente doit être signée entre la Commission scolaire et les usagers énumérant leurs responsabilités respectives ainsi que les procédures à mettre en place advenant le vol ou la perte de l'appareil. Le Service des ressources informatiques est responsable de l'application de cette mesure.

8.7 Protection des actifs de l'information format papier

La Commission scolaire doit se doter d'une directive de protection des actifs de l'information papier. Une notion de bureau propre doit également être instaurée. Ces actifs papier 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 également la gestion des accès physiques aux salles, aux imprimantes ou autres endroits qui détiennent de l'information papier. La protection du périmètre doit être validée à l'aide de tests d'intrusions et les transits d'un endroit à l'autre doivent être encadrés. Chaque direction d'unité administrative est responsable de l'application de cette mesure.

[1] B.Y.O.D. : Bring your own device. Traduction : Prenez vos appareils personnels.

8.8 Gestion des fournisseurs

La Commission scolaire doit se doter d'un processus de gestion de ses fournisseurs pour s'assurer qu'ils ne viendront pas causer des incidents, des divulgations ou pertes de données ou introduire des virus sur son réseau. Pour ce faire, une entente doit être signée avec le fournisseur susceptible d'avoir accès à notre réseau informatique, stipulant qu'il s'engage à répondre aux exigences en cybersécurité de la Commission scolaire et que cette dernière est en droit de voir les résultats des audits effectués sur ce fournisseur. Cette entente doit aussi inclure les objectifs et niveaux de services attendus par ce fournisseur. Les directions d'unités administratives sont responsables de l'application de cette mesure.

9. SENSIBILISATION ET FORMATION

La sécurité de l'information repose notamment sur la régulation des comportements et la responsabilisation individuelle. À cet égard, les employés de la Commission scolaire doivent être formés et conscientisés :

- 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 seront offertes. De plus, des documents explicatifs seront mis à la disposition des personnes touchées par cette politique.

10. CONSÉQUENCES AUX MANQUEMENTS

Tout manquement à cette politique expose l'employé fautif à des mesures administratives ou disciplinaires pouvant aller jusqu'au congédiement. Les fournisseurs, partenaires, invités, consultants ou organismes externes qui contreviennent à cette politique sont également sujets à des sanctions.

11. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le Responsable de la sécurité de l'information (RSI), assisté du comité de travail pour la sécurité de l'information, s'assure de la diffusion et de la mise à jour de la politique.

La *politique relative à la sécurité de l'information* sera révisée périodiquement selon les mises à jour effectuées.

12. CONSULTATION

Comité de gouvernance TIC	Date : 04-04-2019
Comité consultatif de gestion	Date : 17-04-2019
Conseil des commissaires	Date : 30-04-2019

13. ADOPTION

Conseil des commissaires	Date : 30-04-2019

14. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur lors de son adoption par le conseil des commissaires.