



Commission scolaire des
Rives-du-Saguenay

POLITIQUE

(P)-SI-2018-01

Politique sur la sécurité de l'information

Adoptée :	Le 26 juin 2018
En vigueur :	Le 26 juin 2018
Amendement :	
Auteur :	Service informatique

CENTRE ADMINISTRATIF
36, rue Jacques-Cartier Est
Chicoutimi (Québec) G7H 1W2
Téléphone : 418 698-5000

SERVICES ÉDUCATIFS ADULTES
847, rue Georges-Vanier
Chicoutimi (Québec) G7H 4M1
Téléphone : 418 698-5000 p.5213

SERVICE INFORMATIQUE
475, rue Lafontaine, porte 4
Chicoutimi (Québec) G7H 4V2
Téléphone : 418 541-7799

Table des matières

1.	CONTEXTE	3
2.	OBJECTIFS DE LA POLITIQUE.....	3
3.	CADRE LÉGAL ET ADMINISTRATIFS	4
4.	CHAMP D'APPLICATION	5
5.	PRINCIPES DIRECTEURS.....	6
6.	GESTION DES RISQUES.....	6
7.	GESTION DES INCIDENTS	7
8.	DIRECTIVES	7
9.	SENSIBILISATION ET FORMATION	10
10.	SANCTIONS	10
11.	DIFFUSION ET MISE À JOUR DE LA POLITIQUE.....	11
12.	DISPOSITIONS FINALES	11

1. Contexte

La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (R.L.R.Q., chap. G-1.03) et la Directive sur la sécurité de l'information gouvernementale, directive du Secrétariat du Conseil du trésor, applicables à la Commission scolaire des Rives-du-Saguenay, 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 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 (R.S.I.) et un coordonnateur sectoriel de la gestion des incidents (C.S.G.I.) doivent être désignés.

Cette politique permet à la commission scolaire des Rives-du-Saguenay d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue (dont elle est le gardien). Cette information liée aux ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et non numériques (papier, microfilm, microfiche, cassette vidéo, cassette audio, etc.), 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 de la politique

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 que celle-ci 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.*

Par conséquent, la Commission scolaire met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information de la Commission scolaire.

3. Cadre légal et administratifs

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

- *La Loi sur l'instruction publique (R.L.R.Q., c. I-13.3);*
- *La Charte des droits et libertés de la personne (R.L.R.Q., chapitre C-12);*
- *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (R.L.R.Q., c. A-21.1, r.2);*
- *Le Code civil du Québec (R.L.R.Q., chapitre C.C.Q.-1991);*
- *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 (R.L.R.Q., c. G-1.03);*
- *La Loi concernant le cadre juridique des technologies de l'information (R.L.R.Q., chapitre C-1.1);*
- *La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (R.L.R.Q., chapitre A-2.1);*
- *Le Code criminel (L.R.C., 1985, chapitre C-46);*
- *Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (R.L.R.Q., chapitre A-2.1, r. 2);*
- *La Directive sur la sécurité de l'information gouvernementale;*
- *La Loi sur le droit d'auteur (L.R.C., 1985, chapitre C-42);*
- *La politique sur la sécurité dans l'utilisation des technologies de l'information et des télécommunications;*
- *Normes et conditions d'application de la politique sur la sécurité dans l'utilisation des technologies de l'information et des*

- télécommunications;*
- *La politique sur la gestion intégrée de l'information;*
- *La politique sur la sécurité par l'utilisation des systèmes de surveillance vidéo;*
- *Les codes de vie des écoles.*

4. Champ d'application

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à tout le personnel, à toute personne physique ou morale qui à titre de membre du personnel, de membre du Conseil des commissaires, de consultant, de partenaire, de fournisseur, d'étudiant, de titulaire de l'autorité parentale et de la population en général utilise les actifs informationnels de la Commission scolaire

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par la Commission scolaire. À cette fin, il doit :

- *Prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer;*
- *Utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions ou activités, les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés;*
- *Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration 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 son supérieur ou à une personne en autorité de l'organisation tout acte dont il a 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;*

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 non numériques.

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 sécurité de l'information;*
- *Reconnaître que l'environnement technologique des actifs de l'information numérique et non numérique 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 doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;*
- *L'usage des ressources informationnelles par les utilisateurs doit se limiter aux fonctions ou activités qui leur sont attribuées. Une activité personnelle est tolérée tant qu'elle est d'une courte durée. Les informations personnelles ne doivent pas être téléchargées sur le poste par l'utilisateur, car elles pourraient introduire un virus ou programme malveillant et, en conséquence, la Commission scolaire pourrait détruire ces informations ou programmes sans le consentement de l'utilisateur.*

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 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.

Une divulgation au Responsable devrait contenir les informations suivantes :

- *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.*

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 Ministère de l'éducation et des études supérieures 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

Les directives de cette politique sont :

8.1 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 traces pour les audits ultérieurs. Le Service informatique est responsable de l'application de cette mesure pour la gestion numérique. Le Service des ressources matérielles est responsable de l'application de cette mesure pour les accès physiques. Le Service de secrétariat générale est responsable de l'application de cette mesure pour la gestion non numérique. Chaque Direction de service ou d'établissement est responsable des accès logiques aux applications spécifiques de son domaine.

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 et non numérique à son niveau le plus bas possible et diminuer les chances d'une cyberattaque.

Un processus d'analyse des notifications des vulnérabilités venant des fournisseurs doit être mise en place afin de les corriger. Le R.S.I. est responsable 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 R.S.I. est responsable 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 services de cette dernière. Cette stratégie doit être testée à une fréquence adéquate et les écarts corrigés. Le Service informatique 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 vulnérabilité 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 appliquant des stratégies de sécurité à son réseau, la Commission scolaire limite les chances de propagation d'un virus ou d'une attaque. Le Service informatique est responsable de l'application de cette mesure.

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

Une directive sur l'utilisation d'un appareil personnel (tablette numérique, téléphone intelligent, ordinateur portable, etc.) dans l'exercice de ses fonctions ou ses activités doit être élaborée pour bien encadrer cette pratique. Les données de la Commission scolaire doivent être protégées.

Lorsque nécessaire, 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 informatique est responsable de l'application de cette mesure.

8.7 Protection des actifs de l'information format non numérique

La Commission scolaire doit se doter de processus de protection des actifs de l'information non numérique. Une notion de « bureau propre » doit également être instaurée. Ces actifs non numériques peuvent être transportés et produits en plusieurs exemplaires. Les notions de création, d'organisation, de protection, de diffusion et de disposition doivent être considérées dans l'élaboration de ces processus. Les directions d'unités administratives sont responsables de l'application de cette mesure.

8.8 Protection des actifs de l'information numérique

La Commission scolaire doit se doter de processus de protection des actifs de l'information numérique. La notion de classement, d'archivage, de conservation et de destruction doit être considérée dans l'élaboration de ces processus. Les directions d'unités administratives sont responsables de l'application de cette mesure.

8.9 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 ou 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 cette dernière est en droit de voir les résultats des audits effectués (3416, SOC2, etc.) sur ce fournisseur.

Cette entente doit aussi inclure les objectifs ainsi que les niveaux de services attendus par ce fournisseur. Les fournisseurs ont accès à l'information sensible de la Commission scolaire, c'est pourquoi qu'une entente de confidentialité doit être signée avec le fournisseur dans le but de diminuer le risque d'une divulgation de cette information. 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 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.

10. Sanctions

Tout membre du personnel, membre du Conseil des commissaires, consultant, partenaire, fournisseur, étudiant, titulaire de l'autorité parentale et la population en général qui contrevient au cadre légal, au cadre de gestion de la sécurité de l'information ou à la présente politique ainsi qu'aux mesures de sécurité de l'information qui en découlent, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu des lois, des conventions collectives de travail, des politiques et des règlements de la Commission scolaire

11. Diffusion et mise à jour de la politique

Le R.S.I., 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 de sécurité de l'information sera révisée périodiquement selon les mises à jour effectuées.

12. Dispositions finales

La présente politique est entrée en vigueur à la date de son adoption par le conseil des commissaires, soit le 26 juin 2018.