

POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

Responsabilité		Adoptée le
Direction générale		6 octobre 2020
Direction du Service des affaires publiques, des communications et du secrétariat général		Résolution numéro
Direction des Services éducatifs		DG-19/20-58 CA-24/25-32
Direction du Service des ressources financières et du transport scolaire		Révisée le
Direction du Service des ressources humaines		22 avril 2025 – ajustement de la terminologie
Direction du Service des ressources matérielles		Entrée en vigueur le
Direction du Service de la transformation numérique et des ressources informationnelles	√	6 octobre 2020

TABLE DES MATIÈRES

1. PRÉAMBULE	3
2. OBJECTIFS	4
3. CADRE LÉGAL ET ADMINISTRATIF.....	4
4. CHAMP D'APPLICATION	5
5. PRINCIPES DIRECTEURS.....	6
6. DISPOSITION PARTICULIÈRE	6
7. DIFFUSION ET MISE À JOUR DE LA POLITIQUE	6
8. ENTRÉE EN VIGUEUR.....	6

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* (ci-après : « LGGRI ») et de la Directive sur la sécurité de l'information gouvernementale (ci-après : « DSIG »)¹ crée de nouvelles obligations aux centres de services scolaires en leur qualité d'organismes publics.

Alors que la LGGRI assujettit les centres de services scolaires à une nouvelle gouvernance en matière de ressources informationnelles, la DSIG vient en préciser les encadrements. Elles sont appuyées par divers cadres de gestion² émanant du Conseil du trésor. Ces encadrements obligent les centres de services scolaires 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 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. Il est demandé que des mandats soient assignés au sein de chaque centre de services scolaire : un Responsable de la sécurité de l'information et deux (2) Coordonnateurs sectoriels de la gestion des incidents.

Cette politique permet au Centre de services scolaire des Premières-Seigneuries (ci-après : « CSSPS ») d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'il crée ou qu'il collecte dans le cadre de ses activités. Cette information, liée aux ressources humaines, matérielles, pédagogiques, technologiques et financières, est accessible en formats numériques (fichiers) et non numériques (dossiers papiers, formulaires, etc.) dont les risques d'atteinte à sa disponibilité, son intégrité ou sa confidentialité peuvent avoir des conséquences sur :

- 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 du CSSPS et du gouvernement.

¹ Décret 7-2014.

² Cadre gouvernemental de gestion et Cadre de gestion des risques et des incidents à portée gouvernementale.

2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du CSSPS à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information qu'il détient dans le cadre de ses activités, peu importe son support ou ses moyens de communication. Plus précisément, le CSSPS doit veiller à s'assurer de :

- La disponibilité de l'information afin qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées ;
- L'intégrité de l'information afin 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 comporte des renseignements personnels.

Par conséquent, le CSSPS met en place cette politique dans le but d'orienter et de déterminer sa vision. De plus, un cadre de gestion de la sécurité de l'information et des directives de sécurité viendront préciser certains éléments.

3. CADRE LÉGAL

La présente politique s'inscrit principalement dans un contexte régi par :

- La *Loi sur l'instruction publique*, RLRQ, c. I-13.3 ;
- La *Charte des droits et libertés de la personne*, RLRQ, c. C-12 ;
- Le *Code civil du Québec*, RLRQ, c. CCQ-1991 ;
- Le *Code criminel*, L.R.C, 1985, c. C-46 ;
- La *Loi sur le droit d'auteur*, L.R.C, 1985, c. C-42 ;
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 ;
- Le *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques*, RLRQ, c. A-2.1, r.1 ;
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03 ;
- La *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1 ;
- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, RLRQ, c. A-2.1, r. 2 ;
- La Politique-cadre du Conseil du trésor sur la gouvernance et la gestion des ressources informationnelles des organismes publics ;
- La Directive sur la sécurité de l'information gouvernementale (C.T. Décret 7-2014) ;

- La Politique d'utilisation des technologies de l'information et des communications du CSSPS ;
- La Politique relative à la gestion documentaire du CSSPS ;
- Le Code d'éthique applicable aux membres du personnel et à toute personne appelée à œuvrer auprès d'élèves mineurs ou handicapés ;
- Le Cadre de référence relatif aux dossiers de l'élève du CSSPS ;
- Toute autre loi applicable.

4. CHAMP D'APPLICATION

La présente politique s'adresse à tout le personnel, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de bénévole, de fournisseur, d'élève, de parent/tuteur ou de visiteur, utilise les actifs informationnels (actifs numériques et actifs papiers) du CSSPS. Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le CSSPS. À cette fin, il doit :

- a) Utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés ;
- b) 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 ;
- c) Prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer ;
- d) Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister ;
- e) Signaler rapidement à son supérieur immédiat (cadre de qui relève l'employé) ou au Responsable de la sécurité de l'information, 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 du CSSPS.

L'information visée est celle que le CSSPS détient dans le cadre de ses activités, que sa conservation soit assurée directement par lui-même ou par le service d'un tiers. Les formats de l'information visée sont numériques et non numériques.

5. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du CSSPS en matière de sécurité de l'information sont les suivants :

- a) S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité ;
- b) Reconnaître l'importance de la présente politique ;
- c) Responsabiliser les élèves en ce qui a trait à leurs informations personnelles (notion de citoyenneté numérique) ;
- d) Reconnaître que l'environnement technologique des actifs de l'information numérique et non numérique est en changement constant et interconnecté avec le monde ;
- e) Protéger l'information tout au long de son cycle de vie (collecte, utilisation, communication, conservation, destruction) ;
- f) S'assurer que chaque employé n'a accès qu'aux actifs informationnels (applications, droits sur répertoires partagés, documents papiers) requis pour accomplir ses tâches normales ; ce qui correspond à l'attribution des droits d'accès selon le principe directeur du « moindre privilège » ;
- g) Sensibiliser les employés afin qu'ils ne partagent avec d'autres personnes que les informations nécessaires à l'exercice des tâches de celles-ci ;
- h) S'assurer que l'utilisation des actifs de l'information numérique et non numérique par les utilisateurs est encadrée par une politique ou une directive qui explique la procédure appropriée, qui indique ce qui est permis et ce qui ne l'est pas.

6. DISPOSITION PARTICULIÈRE

En cas de manquement à la présente politique, le CSSPS interviendra auprès des personnes concernées et prendra les mesures appropriées, en collaboration avec la direction des ressources humaines.

7. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le Responsable de la sécurité de l'information, assisté du comité de sécurité de l'information, s'assure de la diffusion et de la mise à jour de la politique. Elle sera révisée au besoin.

8. ENTRÉE EN VIGUEUR

La présente politique remplace toute politique antérieure sur le sujet et elle entre en vigueur à la date de son adoption par le conseil d'administration.