

DATE D'APPROBATION : 2019-11-26

RÉSOLUTION NUMÉRO : CC-1920-035

DATE DE RÉVISION :

RÉSOLUTION NUMÉRO :

ENTRÉE EN VIGUEUR : 2019-11-26

RELATIVE À LA SÉCURITÉ DE L'INFORMATION

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) (L.R.Q., chap. G-1.03) et de la Directive sur la sécurité de l'information gouvernementale (DSIG) (C.T. – Décret 7-2014) créent 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 poser les jalons. Ils sont appuyés par divers cadres de gestion émanant du Conseil du trésor et par une approche stratégique. 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 des accès et la gestion des incidents. Ceci demande que 2 rôles soient minimalement comblés au sein de chaque centre de services scolaire : un Responsable de la sécurité de l'information (RSI) et 2 Coordonnateurs sectoriels de la gestion des incidents (CSGI).

Ces encadrements permettent au Centre de services scolaire des Appalaches (CSSA) d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle crée ou collecte dans le cadre de ses activités et dont elle est le gardien. Cette information liée aux ressources humaines, matérielles, pédagogiques, technologiques et financières, est accessible sur des formats numériques et non numériques, dont les risques d'atteinte à sa disponibilité, son intégrité ou sa confidentialité peuvent avoir des conséquences variées 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 centre de services scolaire et du gouvernement.*

Ils mettent en place un cadre permettant de gérer l'information pendant tout son cycle de vie, incluant sa conservation permanente ou sa destruction.

2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du CSSA 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, quels que soient son support ou ses moyens de communication. Plus précisément, le CSSA doit veiller à assurer :

- *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 de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;*
- *La confidentialité de l'information, de façon à limiter l'accès et la divulgation de celle-ci aux seules personnes autorisées à en prendre connaissance, surtout si elle constitue des renseignements personnels.*

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

3. CADRE LÉGAL ET ADMINISTRATIF

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

- *La Loi sur l'instruction publique (L.R.Q., chap. I-13.3);*
- *La Charte des droits et libertés de la personne (L.R.Q., chap. C-12);*
- *Le Code civil du Québec (L.Q., 1991, chap. 64);*
- *La Loi sur les archives (L.R.Q., chap. A-21.1), incluant le Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (r.1);*
- *La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., chap. A-2.1);*
- *La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., chap. G-1.03);*
- *La Politique-cadre 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 télécommunications (SI-P-01).*

4. CHAMP D'APPLICATION

Cette politique vise la gestion intégrée de l'information de la part de tous les utilisateurs.

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

5. DÉFINITIONS

5.1. Utilisateurs

Les utilisateurs sont :

- Tous les employés du CSSA, sans égard à leur horaire de travail, au nombre d'heures de travail ou à leurs années de service continu;
- Les centre de services, stagiaires, consultants, ressources externes et les sous-traitants, durant la période où ils rendent des services au CSSA;
- Les élèves, leurs parents, les membres des différents comités et les bénévoles.

5.2. Actif informationnel

Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles.

Y est également assimilée toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structure de l'information qui y est inscrite.

5.3. Confidentialité

Propriété d'une information accessible aux personnes ou entités désignées et autorisées et divulguée qu'à celles-ci.

5.4. Cycle de vie de l'information

L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation du CSSA.

5.5. Disponibilité

Propriété d'une information accessible aux personnes ou entités désignées et autorisées et divulguée qu'à celles-ci.

5.6. Gestion intégrée de l'information

Gestion de l'ensemble des informations produites ou reçues par le CSSA, peu importe le support sur lequel elles se trouvent (imprimé, technologique, vocal et visuel).

5.7. Incident de sécurité de l'information

Événement aux conséquences néfastes sur la disponibilité, l'intégrité ou la confidentialité de l'information. Il peut être lié ou non à l'usage des technologies de l'information et des communications.

5.8. Information confidentielle

Tout renseignement contenu dans un document détenu par le CSSA, sur quelque support que ce soit, dont la divulgation n'est pas prévue à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., chap. A-21 et, plus particulièrement, les renseignements personnels détenus par le CSSA.

5.9. Intégrité

Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

6. PRINCIPES DIRECTEURS

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

- *Reconnaître l'importance de la sécurité de l'information;*
- *Mettre en place des mesures de sécurité proportionnelles à la valeur de l'information à protéger;*
- *Assurer aux utilisateurs autorisés la disponibilité, l'intégrité et la confidentialité de l'information, et ce, tout au long de son cycle de vie;*
- *S'assurer de bien connaître l'information à protéger, en identifier les détenteurs principaux et leurs caractéristiques de sécurité;*
- *Concevoir, planifier, organiser, élaborer et optimiser les activités relatives à la création, la conservation, la classification, le traitement, l'utilisation, le partage, l'accès, le repérage et la destruction de tous les documents nécessaires aux activités du CSSA, et ce, peu importe le support et la technologie utilisée;*
- *Conscientiser les utilisateurs à une saine gestion des actifs informationnels;*
- *Reconnaître les risques accrus d'une gestion informatisée de l'information et mettre l'accent, par des processus formels, sur la gestion de ces risques, la gestion des accès et la gestion des incidents.*

7. RÔLES ET RESPONSABILITÉS

7.1. Le Conseil d'administration

- *Autorise la Direction générale à procéder à la nomination des responsables prévus à la LGGRI et à la DSIG;*
- *Adopte la présente politique.*

7.2. La Direction générale

- *Veille au respect du cadre gouvernemental de sécurité de l'information;*
- *Procède à la nomination des responsables prévus à la LGGRI et à la DSIG;*
- *S'assure de l'application et du respect de la présente politique dans les établissements et les services administratifs du CSSA.*

7.3. Le Secrétariat général

- *Assiste la Direction générale dans la détermination des orientations stratégiques et des priorités d'intervention en matière de gestion intégrée de l'information et de protection des renseignements personnels;*
- *Élabore, met à jour et diffuse les cadres de gestion, les directives, les guides et les procédures nécessaires à la sécurité de l'information non numérique du CSSA;*
- *Assure le soutien nécessaire aux établissements et aux services administratifs du CSSA dans l'application de la présente politique.*

7.4. Le Service des ressources informatiques

- *Assiste la Direction générale dans la détermination des orientations stratégiques et des priorités d'intervention en matière de sécurité de*

- *l'information numérique;*
- *Élabore, met à jour et diffuse les cadres de gestion, les directives, les guides et les procédures nécessaires à la sécurité de l'information numérique du CSSA;*
- *Assure le soutien nécessaire aux établissements et aux services administratifs du CSSA dans l'application de la présente politique;*
- *Diffuse la politique.*

7.5. Le détenteur de l'information

- *Doit s'assurer de la sécurité de l'information confidentielle du CSSA mise à sa disposition et à la disposition des personnes relevant de leur autorité;*
- *Doit s'assurer que l'accès à l'information confidentielle du CSSA ne soit accessible qu'aux personnes à qui elle est nécessaire à leurs activités.*

7.6. La direction d'établissement et d'un service administratif

- *S'assure de diffuser et de faire connaître la présente politique à l'ensemble des membres de son personnel, de même que les autres écrits de gestion qui en découlent;*
- *S'assure du respect de la politique dans son unité administrative;*
- *Sensibilise les membres de son personnel à la sécurité des actifs informationnels auxquels ils ont accès, aux conséquences d'une atteinte à la sécurité des actifs informationnels, ainsi qu'à leurs rôles et leurs obligations en la matière;*
- *S'assure de l'application des écrits de gestion émis par la Direction générale, le Secrétariat général et le Service des ressources informatiques et matérielles relativement à la présente politique;*
- *Signale promptement tout incident de sécurité de l'information au Secrétariat général (information non numérique) ou du Service des ressources informatiques (information numérique).*

7.7. L'utilisateur

- *Prend connaissance de la présente politique et des écrits de gestion qui en découlent, y adhère et prend l'engagement de s'y conformer;*
- *Utilise les actifs informationnels auxquels il a accès dans le cadre de ses activités dans le respect de la présente politique, de même qu'en harmonie avec les lois, les règlements, les politiques, les procédures, les directives et les autres documents administratifs du CSSA, notamment dans le respect :*
 - *de la protection des renseignements personnels;*
 - *des droits d'auteur et de la propriété intellectuelle.*
- *Protège les actifs informationnels mis à sa disposition en les utilisant avec discernement, aux seules fins prévues et à l'intérieur des accès qui lui sont autorisées;*
- *Signale promptement à son supérieur immédiat tout incident ou anomalie dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité, notamment :*
 - *le vol ou la perte d'informations confidentielles;*
 - *l'intrusion dans un réseau ou un système ou toute autre anomalie pouvant nuire à la protection des actifs informationnels du CSSA.*

8. NON-RESPECT DE LA POLITIQUE

Au regard de sa responsabilité, par le non-respect de la présente politique, tout utilisateur peut s'exposer à des poursuites de nature civile, pénale ou criminelle. Dans le cas des

membres du personnel, un non-respect peut s'accompagner de conséquences, et ce, dans le respect des conventions collectives. Les élèves, quant à eux, s'exposent également aux mesures prévues dans les règles de conduite et de sécurité édictées par leur établissement.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le conseil d'administration.