Centre
de services scolaire
du Chemin-du-Roy
Québec

POLITIQUE

SÉCURITÉ DE L'INFORMATION

- Responsable : **Service des technologies de l'information**
- Date d'adoption : **26 juin 2019**
- Date de la dernière révision : **22 mai 2024** (annule la Politique sur les actifs informationnels adoptée le 11 mai 2011)
- Numéro de référence : **résolution 87-CA/24-05-22**

1. PRÉAMBULE

La présente politique a été adoptée en application du premier alinéa de l'article 12 de la Directive gouvernementale sur la sécurité de l'information. Celle-ci fait obligation aux organismes publics d'adopter et de mettre en œuvre une Politique de sécurité de l'information, de la maintenir à jour et d'en assurer l'application.

2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Centre de services scolaire du Chemin-du-Roy (ci- après appelé « CSSCDR ») de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou son moyen de communication. Plus précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité.

3. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs, c'est-à-dire à tout le personnel, peu importe son statut, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du ministère ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que l'organisme détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

4. CADRE JURIDIQUE

La Politique de 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);
- ✓ 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, chapitre G-1.03);
- ✓ La Loi concernant le cadre juridique des technologies et 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);
- ✓ La Loi sur les archives (LRQ, chapitre A-21.1);
- ✓ La Loi sur l'administration publique (LRQ, chapitre A-6.01);
- ✓ La Loi canadienne sur les droits de la personne (LRC, 1985, chapitre H-6);
- ✓ Le Code criminel (LRC, 1985, chapitre C-46);
- ✓ La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- ✓ Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 02);

- ✓ La Directive gouvernementale sur la sécurité de l'information.

5. DÉFINITIONS

Actif informationnel : Tout document dont la définition correspond à celle de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). À titre de rappel, cette loi définit le document comme étant : « 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 ces formes ou en un autre système de symboles ». Cette même loi assimile au document toutes banques de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

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 de l'organisme public.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

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

6.1 Protection de l'information

a) Le CSSCDR adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale.

b) Le CSSCDR reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, qu'ils doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection, dont les actifs informationnels doivent faire l'objet, est établi en fonction de leur importance, de leur confidentialité, des risques d'accidents, d'erreurs et de malveillance auxquels ils sont exposés.

c) La sécurité des actifs informationnels est soutenue par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

6.2 Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée.

Sont notamment considérés comme confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

6.3 Sensibilisation et formation

L'organisme s'engage, sur une base régulière, à sensibiliser et à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leurs rôles et leurs obligations en la matière.

6.4 Droit de regard

Le ministère exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels.

7. OBLIGATIONS DES INTERVENANTS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

La présente politique fixe les obligations en matière de sécurité de l'information attribuées, notamment au Chef de la sécurité de l'information organisationnelle, aux détenteurs, aux gestionnaires d'unités administratives et aux utilisateurs.

a) Le Chef de la sécurité de l'information organisationnelle: conseille la direction du Centre de services scolaire en ce qui a trait à la détermination des orientations stratégiques et priorités d'intervention en sécurité de l'information et communique, à la demande de la direction générale, les orientations et les priorités d'intervention émanant des instances gouvernementales.
b) Le détenteur de l'information : employé désigné par le CSSCDR, appartenant à la classe d'emploi de niveau-cadre et dont le rôle est, entre autres, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.
c) Les gestionnaires : ils sont chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.
d) Les utilisateurs : ils doivent se conformer aux directives gouvernementales, à la présente politique et aux règles qui leur sont applicables.

Les rôles et responsabilités attribués à d'autres intervenants ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information, sont définis dans le cadre de gestion de la sécurité de l'information, en complément à la présente politique.

8. OBLIGATION DES UTILISATEURS

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

a) 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;

b) 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;

c) 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;

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 immédiatement à son supérieur 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 CSSCDR;

f) Au moment de son départ de l'organisme, remettre les différentes cartes d'identité, cartes d'accès, clés physiques, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de l'exercice de ses fonctions.

9. SANCTIONS

Lorsqu'un utilisateur contrevient à la présente politique ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste.

Les fournisseurs, les partenaires et les fournisseurs externes ou tout autre utilisateur sont également passibles de sanctions.

10. DISPOSITIONS FINALES

a) La présente politique entre en vigueur au moment de son adoption par le conseil d'administration du CSSDR;

b) Le chef de la sécurité de l'information organisationnelle s'assure de la mise en œuvre des dispositions de la présente politique et de ses directives d'application;

c) La présente politique doit être révisée à l'occasion de changements qui pourraient l'affecter;

d) La Cadre de gestion de la sécurité de l'information vient préciser la présente politique. Les obligations qui en découlent sont précisées dans des directives.

11. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à compter du 22 mai 2024.

12. MISE À JOUR

La présente politique doit être mise à jour au plus tard le 22 mai 2029.