
POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Numéro du document : CA 0426-08

Adoptée par la résolution : CA54 0426

En date du : 28 avril 2026


Signature de la direction générale


Signature du secrétaire général

1. PRÉAMBULE

Le Centre de services scolaire de l'Énergie reconnaît que l'information et les technologies qui la supportent sont essentielles à ses opérations courantes et à l'accomplissement de sa mission d'enseignement. Étant donné la valeur administrative, légale et financière de ses actifs informationnels, qui doivent faire l'objet d'une évaluation continue, d'une utilisation et d'une protection appropriée et adéquate tout au long de leur cycle de vie, selon les bonnes pratiques en matière de sécurité informationnelle et avec une approche de gestion des risques, quel qu'en soit le support ou l'emplacement.

L'application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre. G-1.03), de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, 2021, chapitre 25), et de la Directive gouvernementale sur la sécurité de l'information du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics, impose des obligations importantes aux établissements scolaires.

Pour se conformer et répondre à ses obligations réglementaires et légales, le centre de services scolaire de l'Énergie doit adopter, garder à jour et s'assurer de l'application d'une politique de sécurité de l'information pour assurer la mise en place des processus formels de celle-ci afin d'encadrer la gestion des risques, la gestion des accès aux actifs informationnels, la gestion des incidents et la gestion de la continuité des activités.

2. OBJECTIFS

La présente politique constitue le cadre général qui vise la gestion des actifs informationnels dans le respect des droits et obligations du centre de services scolaire pour garantir et répondre aux objectifs de sécurité de l'information et plus spécifiquement pour :

- Assurer la protection de l'actif informationnel tout au long de son cycle de vie, quel que soit le support ou l'emplacement;
- Assurer l'intégrité de l'information en la préservant contre toute destruction, modification et altération de quelque façon sans autorisation;
- Assurer la disponibilité de l'information pour qu'elle soit accessible au moment voulu et utilisable à la demande par l'entité autorisée;
- Préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou divulguée à des personnes, entités ou processus non autorisés;

- Regrouper les lignes directrices, les rôles et les responsabilités des intervenants en sécurité;
- Identifier et classer les actifs informationnels du centre de services scolaire selon leurs degrés de criticités et veiller constamment à leur évaluation ainsi que leur protection adéquate;
- Assurer la conformité aux lois et cadres réglementaires;
- Mettre en place un plan de continuité des activités et de relève informatique;
- Assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements personnels.

3. CADRE DE RÉFÉRENCE

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales.

Fondements légaux :

- La Directive gouvernementale sur la sécurité de l'information [Directive gouvernementale sur la sécurité de l'information](#)
- Cadre gouvernemental de gestion de la sécurité de l'information [Cadre gouvernemental de gestion de la sécurité de l'information](#)
- Aide-mémoire : Politique gouvernementale en cybersécurité [Politique gouvernementale en Cybersécurité - Mesures Clés](#)
- La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1) [Loi concernant le cadre juridique des technologies de l'information](#)
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1) [Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#)
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25) [Aide-Mémoire: Modernisation de la protection des renseignements personnels | Gouvernement du Québec](#)
- Règlement sur les incidents de confidentialité [Règlement sur les incidents de confidentialité](#)

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

- *La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03) [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement](#)
 - Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la *Loi sur la gouvernance et la gestion des ressources informationnelles* [Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la LGGRI](#)
 - Règles relatives à la gestion des projets en ressources informationnelles [Règles relatives à la gestion des projets en ressources informationnelles](#)
 - Règles relatives à la planification et à la gestion des ressources informationnelles [Règles relatives à la planification et à la gestion des ressources informationnelles](#)
 - *La Loi sur les archives* (LRQ, chapitre A-21.1) [Loi sur les archives](#)
 - Les lois sectorielles régissant la mission de chaque organisme
 - La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics
 - Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2) [Règlement sur la diffusion de l'information et sur la protection des renseignements personnels](#)
 - La Charte des droits et libertés de la personne (LRQ, chapitre C-12) [Charte des droits et libertés de la personne](#)
 - Le Code civil du Québec (LQ, 1991, chapitre 64) [Code civil du Québec](#)
 - Le Code criminel (LRC, 1985, chapitre C-46) [Code criminel](#)
 - *Loi sur la fonction publique* (RLRQ, chapitre F-3.1.1) [Loi sur la fonction publique](#)
- Toute autre loi ou règle applicable

Fondements normatifs :

- Le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- Le cadre gouvernemental de gestion de la sécurité de l'information;
- Les normes internationales, notamment ISO 27000 et NIST 800-60;
- Les pratiques gouvernementales en matière de sécurité de l'information.

4. CHAMP D'APPLICATION

PERSONNES VISÉES

Cette politique vise sans exception l'ensemble des personnes physiques et morales, régulières ou occasionnelles, peu importe leur statut, appelées à utiliser les actifs informationnels du centre de services scolaire citant entre autres :

- Le personnel employé du centre de services scolaire;
- Les élèves de notre centre de services scolaire;
- Les partenaires, fournisseurs, contractants et tiers de notre centre de services scolaire.

ACTIFS VISÉS

La politique vise aussi toutes informations et tout actif informationnel :

- Appartenant à notre centre de services scolaire;
- Détenus par un tiers, mais appartenant au centre de services scolaire;
- Utilisés et détenus par un tiers au bénéfice et au nom de notre centre de services scolaire;
- Quel que soit le support de conservation électronique, technologique ou papier.

ACTIVITÉS VISÉES

Cette politique concerne l'ensemble des activités entrant dans le cycle de vie de l'information à savoir : la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation et la destruction des actifs informationnels du centre de services scolaire qu'ils se soient tenus dans le périmètre de ses locaux, dans un autre endroit ou à distance.

5. RÔLES ET RESPONSABILITÉS

La présente politique attribue la gestion de la sécurité de l'information du centre de services scolaire de l'Énergie à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

DIRECTION GÉNÉRALE

La direction générale adopte les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, et les redditions de comptes en matière de sécurité de l'information. Elle assume aussi le processus de délégation des rôles de chef de la sécurité de l'information organisationnelle (CSIO) et du coordonnateur organisationnel des mesures de sécurité de l'information (COMSI).

RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le responsable de la protection des renseignements personnels veille à assurer le respect et la mise en œuvre de la loi sur la protection des renseignements personnels afin de mettre en œuvre des politiques et pratiques encadrant la gouvernance des renseignements personnels.

CHEF DE LA SÉCURITÉ DE L'INFORMATION ORGANISATIONNELLE (CSIO)

La personne assumant la fonction de CSIO est un membre du personnel d'encadrement du centre de services scolaire. Celui-ci se charge de la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. La fonction de CSIO est déléguée par la direction générale. Le CSIO est responsable de la diffusion et de la mise en application de la politique.

COORDONNATEUR ORGANISATIONNEL DES MESURES DE SÉCURITÉ DE L'INFORMATION (COMSI)

Le COMSI agit sur le plan opérationnel. Il intervient dans la mise en œuvre des mesures et apporte le soutien nécessaire au CSIO de l'établissement, notamment en matière de la gestion des incidents et des risques en sécurité de l'information.

Le COMSI représente l'organisme public auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) dans son centre de services scolaire, en soutien au CSIO.

Il collabore auprès du CSIO du centre de services scolaire à l'élaboration des divers éléments stratégiques et tactiques en sécurité de l'information:

- Il maintient le registre des événements et des incidents liés à la sécurité de l'information;
- Il participe et effectue des analyses de risques en sécurité de l'information;
- Il gère le processus de gestion, de déclaration des incidents et de résolution de problème et contribue à sa mise en place;
- Il contribue au processus formel de gestion des droits d'accès à l'information.

DIRECTION DES TECHNOLOGIES DE L'INFORMATION

La direction des technologies de l'information assume la responsabilité de l'application de la présente politique. Elle s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information. De plus, elle participe, avec le CSIO, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du centre de services scolaire, afin d'intégrer des mesures de protection en fonction du niveau de sensibilité de l'information, en tenant compte des exigences réglementaires, d'affaires, légales ou contractuelles.

DIRECTION DES RESSOURCES HUMAINES

En matière de sécurité de l'information, la direction des ressources humaines doit :

- Vérifier, au besoin, les antécédents des candidats à l'embauche et les membres du personnel impliqués dans la sécurité de l'information;
- S'assurer que les responsabilités des intervenants concernant la sécurité de l'information et le respect de la présente politique, ainsi que du cadre normatif des ressources informationnelles, sont inscrites dans les descriptions de tâches des membres du personnel;
- Informer et obtenir de tout nouvel employé du centre de services scolaire son engagement au respect de la présente politique;
- Imposer les sanctions appropriées lors de violation des politiques, règlements, directives et code de conduite touchant à la sécurité de l'information.

RESPONSABLE D'ACTIFS INFORMATIONNELS (DÉTENTEUR)

Le responsable d'actifs informationnels est le cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il ou elle :

- Participe à la catégorisation de l'information de l'unité sous sa responsabilité et à l'analyse de risques;
- Veille à la protection de l'information et des systèmes d'information en conformité avec la politique de sécurité de l'information;
- Rapporte tout événement ou toute menace liée à la sécurité de l'information;
- Collabore à la mise en œuvre de toute mesure pour améliorer la sécurité de l'information afin de remédier à un incident au besoin.

UTILISATRICES ET UTILISATEURS

La responsabilité de la sécurité de l'information de notre centre de services scolaire incombe à toutes les utilisatrices et à tous les utilisateurs des actifs informationnels. L'utilisatrice ou utilisateur qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à la protéger.

À cette fin, l'utilisatrice ou l'utilisateur doit :

- Se conformer à la présente politique et à toute autre directive du centre de services scolaire en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- Être responsable des actions résultant de l'usage de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers, à moins qu'il démontre que les actions posées par un tiers ne découlent pas d'une négligence ou d'une malveillance de sa part;
- Aviser une personne responsable, un enseignant ou son supérieur immédiat, de toute situation susceptible de compromettre la sécurité de l'actif informationnel;
- Au besoin, participer à la catégorisation de l'information de son service;
- Utiliser les droits d'accès qui lui sont attribués et autorisés, de l'information et des systèmes d'information qui sont mis à sa disposition, uniquement dans le cadre approprié à son utilisation et aux fins auxquelles ils sont destinés;

- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- Collaborer à toute intervention visant à indiquer ou à mitiger une menace ou un incident à la sécurité de l'information.

CADRE DE GESTION

La mise en œuvre de la présente politique s'appuie sur la définition d'un cadre de gestion en sécurité de l'information qui précise le champ d'action des différents intervenants. Le cadre de gestion précise l'organisation fonctionnelle en matière de sécurité de l'information et rend possible la définition d'objectifs clairs et une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information sont réévaluées de manière périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces et des risques.

La politique de sécurité de l'information du centre de services scolaire se base sur cinq axes fondamentaux de gestion, comme suit :

GESTION DES IDENTITÉS ET DES ACCÈS (GIA)

La gestion des accès est encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de toute information détenue par le centre de services scolaire soient strictement réservés aux personnes autorisées pour protéger la confidentialité.

GESTION DES VULNÉRABILITÉS

La gestion des vulnérabilités se caractérise par un déploiement des mesures pour maintenir à jour les logiciels du parc informatique afin de garder les vulnérabilités au niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une gestion de notification des vulnérabilités venant des fournisseurs ou des prestataires de services doit être en place pour qu'elles soient évaluées et corrigées le cas échéant.

GESTION DU RISQUE

La gestion du risque touchant l'actif informationnel du centre de services scolaire est basée sur une analyse des menaces encourues liées à l'intégrité, la disponibilité et la confidentialité de l'information détenue par le centre de services scolaire. De cette analyse découlent des directives liées à l'utilisation et l'opération des systèmes d'information ainsi qu'aux résultats escomptés.

GESTION DES INCIDENTS

La gestion des incidents se caractérise par la mise en place de procédures de compte rendu, d'analyse relativement aux incidents de sécurité et de mesures correctives pour y donner suite. Les mesures déployées visent à assurer la continuité des services. Dans la gestion des incidents, le centre de services scolaire peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'actif informationnel.

GESTION DE LA REPRISE ET DE LA CONTINUITÉ DES AFFAIRES

La gestion de la reprise et de la continuité des affaires se caractérise par la mise en place des processus pour identifier les incidents opérationnels majeurs susceptibles de menacer le centre de services scolaire tels les catastrophes naturelles, les pannes d'électricité ou de télécommunication, les pannes informatiques, le piratage, le terrorisme, les pandémies, etc.

L'identification de ces incidents permet d'évaluer leurs impacts sur les activités de l'établissement et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

FORMATION, SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur l'adoption de comportements sécuritaires et la responsabilisation individuelle.

À cet égard, les membres du personnel du centre de services scolaire doivent être sensibilisés :

- À la sécurité de l'information et des systèmes d'information du centre de services scolaire;
- Aux conséquences d'une atteinte à la sécurité des actifs informationnels;
- À leur rôle et à leurs responsabilités en la matière.

Le centre de services scolaire 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 la sécurité de ces actifs ainsi qu'à leur rôle et leurs obligations en la matière. L'utilisateur a la responsabilité de participer à ces activités de sensibilisation et de formation. Par ailleurs, le centre de services scolaire favorise le recours aux services communs de formation en sécurité de l'information.

ÉNONCÉ DES PRINCIPES GÉNÉRAUX

PROTECTION DE L'INFORMATION¹

- Disponibilité

La disponibilité garantit que les utilisateurs autorisés d'un système ont un accès opportun et ininterrompu aux informations contenues dans ce système ainsi qu'au réseau. Les informations doivent être accessibles en temps utile et de la manière requise par un utilisateur autorisé. Afin d'aider à assurer cette disponibilité, des mesures de contrôles doivent être mises en place.

- Intégrité

L'intégrité des données consiste à garantir que les données n'ont été modifiées d'aucune façon au cours de leur communication, qu'il s'agisse de données au repos, en transit ou en mémoire. Afin d'assurer l'intégrité des données, des mesures de sécurité physiques et d'accès logiques doivent être mises en place.

- Confidentialité

La confidentialité vise à empêcher tout accès non autorisé à des informations sensibles. Elle a pour but de s'assurer qu'une information ou une donnée est accessible uniquement par les personnes autorisées. La confidentialité de l'information doit aussi être assurée tout au long de son cycle de vie. Afin de garantir la confidentialité, des mesures de contrôles doivent être mises en place.

CATÉGORISATION DE L'INFORMATION

L'information constitue une ressource essentielle qui doit être protégée tout au long de son cycle de vie, raison pour laquelle il est primordial de garder à jour l'inventaire de l'ensemble des actifs informationnels de l'organisation. L'un des premiers intrants de la sécurité de l'information est la connaissance de la sensibilité de l'information des actifs informationnels d'une organisation. La catégorisation des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des actifs dans le but d'en déterminer le niveau de protection.

Il est important de réévaluer la catégorisation des actifs informationnels sur une base périodique pour s'assurer que la catégorisation attribuée est toujours appropriée en fonction des modifications des obligations légales et contractuelles, ainsi que des

¹ [Publication NIST SP800-53](#)

changements dans l'utilisation des données ou leur valeur pour l'établissement. Cette évaluation devrait être effectuée par le détenteur de l'actif.

6. SANCTION

En cas de non-respect à la présente politique, l'utilisateur engage sa responsabilité personnelle; il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information ne soit pas protégée adéquatement.

Tout membre du personnel du centre de services scolaire qui contrevient au cadre légal, à la présente politique et 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 de la loi, des règles administratives internes ainsi que des conventions collectives applicables.

De même, tout non-respect à la présente politique, qu'il soit perpétré par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant à notre centre de services scolaire ou en vertu des dispositions de la législation applicable en la matière.

7. RÉVISION

De manière à suivre l'évolution du cadre de référence applicable et des besoins du Centre, la présente politique pourra être mise à jour au besoin, au plus tard tous les 3 à 5 ans.

8. ENTRÉE EN VIGUEUR

La présente politique a été adoptée par le Conseil d'administration par la résolution CA54 0426 et entre en vigueur le jour de son adoption. Elle remplace et abroge la politique sur la sécurité de l'information adoptée par résolution numéro 92 1218 le 18 décembre 2018.

9. HISTORIQUE DES REVISIONS

Dernière mise à jour : 18 décembre 2018, résolution 92 1218