



Politique n° 2023-CA-28 :	<i>Politique relative à la sécurité de l'information</i>
----------------------------------	---

Adoptée :	Résolution n°
Mise à jour :	Résolution n°
Origine :	Secrétariat général

NOTE : Fidèle à son engagement pour le respect de la diversité, la Commission scolaire Sir-Wilfrid-Laurier utilise un langage inclusif dans toutes ses communications écrites. Lorsque l'utilisation d'une formulation neutre s'avère difficile, le masculin générique est utilisé uniquement à des fins de clarté et de lisibilité.

1.0 CONTEXTE

Dans le cadre de ses activités, la Commission scolaire Sir-Wilfrid-Laurier (ci-après appelée la CSSWL) traite une grande quantité de données dans de nombreux formats. Étant donné la nature de ces données, la CSSWL doit s'assurer qu'elles sont traitées de manière appropriée. La CSSWL doit mettre en place une série de mesures pour assurer une gestion appropriée et souple de l'information détenue, et pour se conformer à diverses obligations légales et réglementaires. À cet égard, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, loi 133) et la *Directive sur la sécurité de l'information gouvernementale* (DSIG, une directive du Secrétariat du Conseil du trésor du Québec applicable aux commissions scolaires et aux centres de services scolaires) imposent des obligations aux établissements d'enseignement en leur qualité d'organismes publics. Notamment, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* et la DSIG exigent que les commissions scolaires et les centres de services scolaires adoptent, mettent en œuvre, mettent à jour et fassent respecter une *Politique relative à la sécurité de l'information* (ci-après appelée la Politique) pour assurer la confidentialité, l'intégrité et la disponibilité de l'information qu'ils conservent ou utilisent dans le cadre de leurs activités.

2.0 OBJECTIFS

Cette politique vise à promouvoir les pratiques exemplaires et à sensibiliser les parties prenantes de la CSSWL de manière à nous conformer aux exigences réglementaires et réduire les risques tout en protégeant l'information que nous conservons, transférons et utilisons. La CSSWL souhaite réitérer son engagement et ses efforts continus pour assurer la confidentialité, l'intégrité et la disponibilité de l'information. À cet égard, la présente Politique vient s'ajouter à la politique *Utilisation des ressources des technologies de l'information et de la communication* de la CSSWL qui affirme notamment notre engagement à fournir et maintenir une infrastructure de technologie de l'information sécurisée, efficace et fiable.

3.0 CADRE DE RÉFÉRENCE

- *Charte des droits et libertés de la personne* (RLRQ, c. C-12)
- *Loi sur l'instruction publique* (RLRQ, c. I-13.3)

- *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (RLRQ, c. A-21.1, r.1)
- *Code civil du Québec* (LQ, 1991, c. 64)
- *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, loi 133)
- *Loi concernant le cadre juridique des technologies de l'information* (LRQ, c. C-1.1)
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1)
- *Code criminel* (LRC, 1985, c. C-46)
- *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (c. A-2.1, r. 2)
- *Directive sur la sécurité de l'information gouvernementale*
- *Loi sur le droit d'auteur* (LRC, 1985, c. C-42).
- Politique n° 2000-IT-01 : *Utilisation des ressources des technologies de l'information et de la communication* de la CSSWL
- Politique n° 2018-CA-23 : *Politique régissant la divulgation d'actes répréhensibles* de la CSSWL
- Politique n° 2011-HR-08 : *Code de conduite du personnel* de la CSSWL
- Règlement n° BL2009-CA-17 : *Code d'éthique et de déontologie applicable aux commissaires de la Commission scolaire Sir-Wilfrid-Laurier*
- Politique n° 2005-CA-12 : *Politique de communication* de la CSSWL

4.0 PORTÉE

Cette politique s'applique en tout temps à toutes les personnes qui utilisent de l'information de la CSSWL (membres du personnel, jeunes et adultes, élèves du secteur de la formation professionnelle, commissaires, conseillères et conseillers, parents, partenaires, bénévoles, fournisseurs) et qui ont accès et/ou utilisent des actifs informationnels de la CSSWL, peu importe le format de stockage, les moyens utilisés pour créer ces actifs informationnels, y accéder et/ou les transmettre, l'endroit depuis lequel on accède, sauvegarde et/ou transmet ces actifs informationnels, et que ces actifs informationnels soient ou non gérés ou détenus par la CSSWL ou une tierce partie.

5.0 PRINCIPES DIRECTEURS

Les principes directeurs suivants régissent les mesures que la CSSWL prendra en ce qui concerne la sécurité de l'information :

- 5.1 Développer une compréhension complète de l'information qui doit être protégée;
- 5.2 Reconnaître l'importance de la présente politique;
- 5.3 Comprendre que l'environnement technologique des actifs informationnels numériques et non numériques change continuellement;
- 5.4 Protéger l'information tout au long de son cycle (création, traitement, destruction);

- 5.5 S'assurer que les membres du personnel ont uniquement accès à l'information nécessaire pour exercer normalement leurs fonctions;
- 5.6 L'utilisation d'actifs informationnels numériques et non numériques doit être régie par une politique ou une directive qui explique la procédure appropriée à suivre et établit ce qui est permis et ce qui ne l'est pas.

6.0 SENSIBILISATION ET FORMATION

La sécurité de l'information dépend en grande partie de l'encadrement de la conduite personnelle et de la responsabilisation individuelle. Pour cette raison, les membres de la communauté de la CSSWL doivent suivre une formation concernant ce qui suit, et/ou en être informés :

- la sécurité de l'information et les systèmes informatiques de la CSSWL;
- les directives en matière de sécurité;
- la gestion des risques;
- la gestion des incidents;
- les menaces existantes;
- les conséquences d'une brèche de sécurité;
- le rôle et les responsabilités du personnel en matière de sécurité.

7.0 COMITÉS

7.1 Comité sur la sécurité de l'information et l'accès à l'information et la protection des renseignements personnels

Parmi les obligations en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, le comité sur la sécurité de l'information et l'accès à l'information et la protection des renseignements personnels (ci-après appelé le Comité) sera également responsable d'exercer ses responsabilités à l'égard de la protection et l'accès des renseignements personnels. Le Comité sera également responsable de la mise en œuvre de cette politique et créera le cadre de gestion qui énoncera les responsabilités du Comité.

Le Comité est composé des membres suivants :

- directrice ou directeur du Service des affaires corporatives, juridiques et des communications;
- directrice adjointe ou directeur adjoint – Service des affaires juridiques, corporatives et des communications;
- directrice ou directeur – Service des ressources informationnelles;
- coordonnatrice ou coordonnateur – Service des ressources informationnelles;
- régisseuse ou régisseur – Service des ressources informationnelles;
- coordonnatrice ou coordonnateur – Service des ressources humaines;
- bibliothécaire – Service des affaires corporatives, juridiques et des communications;
- des personnes représentant d'autres services peuvent être invitées lorsque cela s'avère pertinent.

7.2 Équipe de gestion des crises

Une équipe de gestion des crises est créée pour assurer une intervention appropriée lors d'incidents majeurs et assurer la continuité des opérations de la CSSWL dans de telles circonstances. L'équipe de gestion des

crises collaborera avec le comité sur la sécurité de l'information et l'accès à l'information et la protection des renseignements personnels, au besoin.

L'équipe de gestion des crises en lien avec la sécurité de l'information est composée des membres suivants :

- la direction générale ou une personne déléguée;
- les coordonnatrices organisationnelles ou coordonnateurs organisationnels des mesures de sécurité de l'information;
- la personne responsable de la sécurité de l'information;
- une personne représentant l'équipe des communications;
- tout autre membre de l'équipe de gestion dont le service/l'école/le centre est affecté par l'incident de sécurité de l'information.

8.0 SANCTIONS

Tout membre du personnel de la CSSWL qui contrevient au cadre juridique, à la présente politique ou aux mesures de sécurité de l'information qui en découlent, est passible de sanctions en fonction de la nature, de la sévérité et des conséquences de la contravention, comme prescrit par la loi applicable ou les règlements disciplinaires internes (y compris ceux stipulés dans les conventions collectives, les politiques et les règlements de la CSSWL, de même que le *Code de conduite du personnel de la CSSWL*). Les élèves, fournisseurs, partenaires, personnes invitées, conseillères et conseillers, et organisations externes sont passibles de sanctions jugées appropriées par la CSSWL.

9.0 DISTRIBUTION ET MISES À JOUR

La présente politique doit être révisée périodiquement pour évaluer son efficacité, et elle doit être mise à jour en conséquence.

10.0 CADRE DE GESTION

Un cadre de gestion sera établi par le comité sur la sécurité de l'information et l'accès à l'information et la protection des renseignements personnels afin de définir les rôles et les responsabilités des parties prenantes de la CSSWL concernant la présente politique, ainsi que pour dresser la liste des mesures qui favoriseront la sécurité, l'intégrité et la confidentialité de l'information. Ce cadre de gestion sera mis à jour régulièrement par le Comité compte tenu de la nature évolutive de l'environnement numérique.

11.0 DATE D'ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil des commissaires.