COMMISSION SCOLAIRE
DES TROIS-LACS

**POLITIQUE Nº 16-19-03-02**

# CAHIER DE GESTION

## POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

| **Responsabilité** | |
|---|---|
| Direction générale | |
| Service du secrétariat général et des communications | |
| Services éducatifs aux jeunes | |
| Service des ressources humaines et de l'organisation scolaire | |
| Service des ressources financières et du transport | |
| Service des ressources matérielles et des bâtiments communautaires | |
| Service des technologies de l'information | ✓ |
| Établissements | |

| **Entrée en vigueur** |
|---|
| **2019-03-12** |
| **Résolution numéro** |
| **CC 19-03-81** |
| **Amendement** |
| |

# TABLE DES MATIÈRES

## 1. CONTEXTE

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) (RLRQ, chapitre G-1.03)* et de la *Directive sur la sécurité de l'information gouvernementale (DSIG)* (une directive du Conseil du trésor du Québec applicable à la Commission scolaire) créent des obligations aux établissements scolaires en leur qualité d'organismes publics.

Ainsi, la *DSIG* oblige la Commission scolaire 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 gouvernementale – 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. Ceci demande que deux (2) rôles soient comblés au sein de chaque commission scolaire. Tel qu'il est stipulé dans le *Guide de nomination*, un Responsable de la sécurité de l'information (RSI) et deux (2) Coordonnateurs sectoriels de la gestion des incidents (CSGI) doivent être désignés.

Cette politique permet à la Commission scolaire des Trois-Lacs (Commission scolaire) d'accomplir ses missions, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue (dont elle est le gardien). Cette information liée aux ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et non numériques, dont les risques d'atteinte à sa disponibilité, intégrité ou confidentialité peuvent avoir des conséquences liées à :

- 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 de la Commission scolaire et du gouvernement.

## 2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement de la Commission scolaire à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, la Commission scolaire doit veiller à :

- 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 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 constitue des renseignements personnels.

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

## 3. CADRE LÉGAL ET ADMINISTRATIF

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

- la *Charte des droits et libertés de la personne (RLRQ, chapitre C-12)*;
- la *Loi sur l'instruction publique (RLRQ chapitre I-13.3)*;
- la *Loi sur les archives (chapitre A-21.1)*;
- 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 (RLRQ, chapitre G-1.03)*;
- la *Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C-1.1)*;
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1)*;
- le *Code criminel (LRC, 1985, chapitre C-46)*;
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2)*;
- la *Directive sur la sécurité de l'information gouvernementale*;
- la *Loi sur le droit d'auteur (LRC, 1985, chapitre C-42)*;
- la *Politique d'utilisation des technologies de l'information, du réseau des télécommunications et des médias sociaux.*

## 4. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à tout le personnel, à toute personne physique ou morale qui à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public utilise les actifs informationnels de la Commission scolaire. Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par la Commission scolaire. 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 de la Commission scolaire.

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

## 5. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions de la Commission scolaire 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 politique de sécurité de l'information;

c) reconnaître que l'environnement technologique des actifs de l'information numérique et non numérique est en changement constant et interconnecté avec le monde;

d) protéger l'information tout au long de son cycle de vie (création, traitement, destruction);

e) s'assurer que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;

f) l'utilisation des actifs de l'information numérique et non numérique par les utilisateurs doit être encadrée par une politique ou directive qui explique une marche à suivre appropriée, qui indique ce qui est permis et ce qui ne l'est pas.

## 6. GESTION DES RISQUES

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

La gestion des risques liés à la sécurité de l'information numérique et non numérique s'inscrit dans le processus global de gestion des risques de la Commission scolaire. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*. L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement de la Commission scolaire.
Le niveau de protection de l'information est établi en fonction :

- de la nature de l'information et de son importance;
- des probabilités d'accident, d'erreur ou de malveillance auxquelles elles sont exposées;
- des conséquences de la matérialisation de ces risques;
- du niveau de risque acceptable par la Commission scolaire.

## 7. GESTION DES INCIDENTS

La Commission scolaire déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, elle met en place les mesures nécessaires à l'obtention des buts suivants :

- limiter l'occurrence des incidents en matière de sécurité de l'information;
- gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés au *ministère de l'Éducation et de l'Enseignement supérieur* conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Dans la gestion des incidents, la Commission scolaire peut exercer ses pouvoirs et ses prérogatives en égard de toute utilisation inappropriée de l'information qu'elle détient ou de ses systèmes d'information.

## 8. DIRECTIVES

Pour chacune des directives élaborées ci-dessous, prévoir une révision à fréquences prédéterminées et procéder à une mise à jour au besoin.

A. Gestion des accès
Une gestion des accès logique et physique doit être élaborée, encadrée et contrôlée pour faire en sorte de protéger la disponibilité, l'intégrité et la confidentialité de l'information numérique et non numérique. Cette gestion doit inclure l'approbation, la revalidation et la destruction de ces accès et la conservation de ces évidences pour les audits ultérieurs.

B. Gestion des vulnérabilités
La Commission scolaire déploie des mesures pour maintenir à jour son parc informatique afin de maintenir les vulnérabilités des actifs de l'information numérique et non numérique à son niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une mesure de notification des vulnérabilités venant des fournisseurs doit être mise en place pour les corriger.

C. Gestion des copies de sauvegardes
La Commission scolaire doit élaborer une stratégie de copie de sauvegarde pour se prémunir contre une perte de données numériques et non numériques. Cette stratégie doit inclure la rétention des copies, les alertes d'erreurs lors de la prise de copie et les tests de restauration de ces copies à une fréquence adéquate.

D. Continuité des affaires
La Commission scolaire doit élaborer une stratégie de continuité des affaires advenant qu'un incident cause l'arrêt de la prestation de service d'une commission scolaire. Cette stratégie doit être testée à une fréquence adéquate et les écarts corrigés.

E. Protection du périmètre du réseau
La Commission scolaire doit instaurer des exercices de tests d'intrusion et balayages de vulnérabilités pour identifier les points d'entrées susceptibles de donner un accès

inapproprié à des individus ou des programmes malicieux. De plus, un système de prévention et de détection d'intrusion devrait être mis en place pour augmenter le niveau de protection. Aussi, segmenter son réseau permet à la Commission scolaire de diminuer les chances de propagation d'un virus ou d'une attaque.

F. Utilisation d'un appareil personnel (B.Y.O.D.)

Une directive sur l'utilisation d'un appareil personnel (tablette numérique, téléphone intelligent, etc.) dans l'exercice de ses fonctions doit être élaborée pour bien encadrer cette pratique. Les données de la Commission scolaire doivent être protégées.

Une entente doit être signée entre les parties énumérant leurs responsabilités respectives et qu'advenant le vol ou la perte de l'appareil, la Commission scolaire doit procéder à l'effacement de ses données.

G. Protection des actifs de l'information format non numérique

La Commission scolaire doit se doter d'une directive de protection des actifs de l'information non numérique qui sont en lien principalement avec les classeurs et imprimantes. Une notion de bureau propre doit être instaurée. Ces actifs non numériques peuvent être transportés et produits en plusieurs exemplaires. La notion d'archivage et de destruction doit être considérée dans l'élaboration de cette directive. Cette protection inclut la gestion des accès physiques aux salles, aux imprimantes ou aux autres endroits qui détiennent des actifs de l'information non numérique. Cette directive de la protection du périmètre prévoit faire des tests d'intrusions ainsi que de les protéger lors du transit d'un endroit à un autre.

H. Gestion des fournisseurs

La Commission scolaire doit mettre en place un processus de gestion de ses fournisseurs pour s'assurer qu'ils ne viendront pas causer des incidents, des divulgations/pertes de données ou introduire des virus sur son réseau. Pour ce faire, une entente doit être signée avec le fournisseur qui stipule qu'il s'engage à répondre aux exigences en cybersécurité de la Commission scolaire et que la Commission scolaire est en droit de voir les résultats des audits (3416, SOC2, etc.) conduits sur ce fournisseur. Cette entente doit aussi inclure les objectifs/niveaux de services attendus par ce fournisseur. Les fournisseurs ont accès à l'information sensible de la Commission scolaire, c'est pourquoi une entente de confidentialité doit être signée avec le fournisseur dans le but de diminuer le risque d'une divulgation de cette information.

## 9. SENSIBILISATION ET FORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté de la Commission scolaire doivent être formés et sensibilisés :

- à la sécurité de l'information et des systèmes d'information de la Commission scolaire;
- aux directives de la sécurité;
- à la gestion des risques;
- à la gestion des incidents;
- aux menaces existantes;
- aux conséquences d'une atteinte à la sécurité;
- à leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. De plus, des documents explicatifs sont disponibles sur le site Internet de la Commission scolaire.

## 10. SANCTIONS

Tout employé de la Commission 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 ou des règles disciplinaires internes applicables (dont celles des conventions collectives de travail et des *Règlements de la Commission scolaire*).

Les fournisseurs, partenaires, invités, consultants ou organismes externes sont passibles de ces sanctions.

## 11. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le RSI, assisté du comité de travail pour la sécurité de l'information, s'assure de la diffusion et de la mise à jour de la politique. La politique de sécurité de l'information sera révisée périodiquement selon les mises à jour effectuées.

## 12. ENTRÉE EN VIGUEUR

La présente politique est entrée en vigueur à la date de son adoption par le conseil des commissaires, soit le 12 mars 2019.