COMMISSION SCOLAIRE DES SOMMETS

RÈGLEMENTS, POLITIQUES ET PROCÉDURES

POLITIQUE

SUR LA

SÉCURITÉ DE L'INFORMATION

DE LA

COMMISSION SCOLAIRE DES SOMMETS

2019-06-25	117

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) (LRQ, Loi 133) 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.

Cette politique permet à la commission scolaire d'accomplir sa mission, 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. DÉFINITIONS

Actif informationnel

Ce terme désigne tant l'information consignée dans un document que le système qui permet de la prendre en charge. L'actif informationnel peut être constitué de documents technologiques ou de documents en format papier ou encore d'une banque de données. Il peut s'agir aussi d'une technologie de l'information, d'une installation, d'un bien informatique ou d'un ensemble de ces éléments.

Catégorisation des actifs informationnels

La catégorisation des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des renseignements que détient la CSS, dans le but d'en déterminer le niveau de protection, eu égard aux risques potentiels aux chapitres de la disponibilité, de l'intégrité, de la confidentialité, de l'authentification et de l'irrévocabilité.

La CSS peut ainsi tenir compte du degré de sensibilité déterminé de ses actifs informationnels pour mettre en œuvre les mesures lui permettant de se conformer à ses obligations légales, d'éviter des pertes financières, d'atteindre ses objectifs en ce qui a trait à la prestation de services et de rehausser la confiance des citoyens et des entreprises à l'égard de ses services et des services publics, en général.

La catégorisation d'un actif informationnel sert donc de base pour sécuriser le support sur lequel les renseignements sont conservés : papier, numérique, enregistrement, audiovisuel, etc.

Cycle de vie de l'information

Le cycle de vie de l'information consiste en l'ensemble des étapes que franchit une information depuis 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 la CSS.

Document

Ce terme désigne un ensemble constitué d'information qui se trouve sur un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support, et est intelligible sous forme de mots, de sons ou d'images. Elle peut être communiquée au moyen de quelque mode d'écriture que ce soit, y compris un système de symboles transcrits sous l'une de ces formes. Est assimilée à un document, toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Gestion des incidents

Le processus de la gestion des incidents permet de préparer l'organisation en vue de la prise en charge d'incidents susceptibles de compromettre la sécurité de l'information, depuis cette prise en charge jusqu'au retour à la normale. Il prévoit, le cas échéant, l'escalade jusqu'aux autorités ministérielles ou gouvernementales. Il prévoit également l'arrimage avec d'autres processus de la CS, dont le plan local des mesures d'urgence.

Incident touchant la sécurité de l'information à portée gouvernementale

Ce terme désigne une conséquence observable de la concrétisation d'un risque quant à la sécurité de l'information à portée gouvernementale. Une intervention concertée sur le plan gouvernemental est alors nécessaire.

Règle

Sous ce terme général sont compris la présente politique, les cadres de gestion et directives à venir ainsi que les lois et les règlements en vigueur, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et le Code criminel.

Renseignements personnels et confidentiels

L'article 54 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) indique ce qui suit : « Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier ».

La Commission d'accès à l'information du Québec a précisé les trois critères énoncés dans cet article et permettant d'établir qu'un renseignement est personnel ou non :

- Il doit s'agir d'un *renseignement* (l'information doit faire connaitre quelque chose) ;
- Le renseignement doit *concerner* (avoir trait à) une personne physique ;
- Il doit permettre d'*identifier* cette personne (de la reconnaitre par rapport à quelqu'un d'autre ou à différentes classes ou catégories d'individus, ou encore de reconnaitre sa nature).

Sécurité physique

La sécurité physique concerne la protection de l'accès physique à des lieux, à de l'équipement, à du matériel, à des documents et à des personnes.

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 (LRQ, chapitre C-12) ;
- La loi sur l'instruction publique (L.R.Q. c. I-13.3) ;
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (L.R.Q. c. A-21.1, r.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 (LRQ, chapitre G-1.03) ;
- La Loi concernant le cadre juridique des technologies de 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) ;
- Le Code criminel (LRC, 1985, chapitre C-46) ;
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RRQ, 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 Loi sur les archives (LRQ, A-21.1) ;
- La politique sur l'utilisation des ressources informationnelles (116).

4. CHAMP D'APPLICATION

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

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

5. 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.

6. PRINCIPES GÉNÉRAUX

Les principes qui guident les actions de la commission scolaire en matière de sécurité de l'information sont les suivants :

a) Reconnaitre l'importance de la politique de sécurité de l'information ;

b) S'assurer de bien connaitre l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité ;

c) Reconnaitre que l'environnement technologique des actifs informationnels est en changement constant et interconnecté avec le monde ;

d) Protéger le cycle de vie de l'information ;

e) S'assurer que chaque employé ait accès au minimum d'information requis pour accomplir ses tâches normales (caractère de nécessité) ;

f) Encadrer par une directive l'utilisation des actifs informationnels par les utilisateurs ;

g) Sensibiliser et former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

7. RÔLES ET RESPONSABILITÉS

Conseil des commissaires

Le conseil des commissaires nomme le responsable en sécurité de l'information et le coordonnateur sectoriel de la gestion des incidents dans la commission scolaire et adopte la politique de sécurité de l'information ainsi que toute modification à celle-ci.

Direction générale

La Direction générale de la commission scolaire est première responsable de la sécurité de l'information. À ce titre, elle veille au respect du cadre gouvernemental de sécurité de l'information et s'acquitte de ses obligations telles qu'elles sont édictées dans la Directive sur la sécurité de l'information gouvernementale.

Comité pour la sécurité de l'information

Le comité pour la sécurité de l'information a pour objectif d'assister le responsable de la sécurité de l'information (RSI) à mettre en place le cadre de gestion de la sécurité de l'information et autre élément pouvant être nécessaire pour assurer la protection de la commission scolaire et être conforme à la règlementation.

Responsable de la sécurité de l'information (RSI)

Le RSI est nommé par le Conseil des commissaires. Il relève du directeur général au sens du Cadre gouvernemental de gestion de la sécurité de l'information. Ses principales responsabilités sont :

- Conseiller la haute direction sur les orientations stratégiques ;
- Assurer la coordination et la cohérence des actions de la sécurité de l'information (SI) menées au sein de sa commission scolaire par tous les intervenants ;
- Communiquer et coordonner la mise en œuvre des processus ;
- Voir à la reddition de compte ;
- Établir des liens avec les autres RSI.

Coordonnateur sectoriel de la gestion des incidents (CSGI)

Le CSGI apporte son soutien au RSI, notamment en ce qui a trait à la gestion des incidents et des risques en sécurité de l'information. Ses principales responsabilités sont :

- Mettre en œuvre les processus SI ;
- Contribuer aux analyses des risques de la SI (ex. : exposition aux cyberattaques) ;
- Coordonner la gestion d'incidents à portée gouvernementale ;
- Procéder à l'autoévaluation de la sécurité des systèmes informatiques de sa commission scolaire ;
- Maintenir une veille continue sur les risques, les menaces et les vulnérabilités ;
- Maintenir un lien avec les autres CSGI.

Service des technologies de l'information

Le service des technologies de l'information est responsable de l'élaboration et du maintien d'outils qui sont conformes aux objectifs de la commission scolaire en matière de sécurité de l'information. Il élabore et met en œuvre des projets de développement ou d'acquisition des systèmes d'information. Il participe aux analyses de risque et voit à anticiper les menaces à la sécurité des systèmes

d'information. Il prend toutes les mesures nécessaires pour contrer les menaces ou tout incident en matière de sécurité de l'information. Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par le directeur général.

Service des ressources matérielles

Le service des ressources matérielles participe, avec le CSGI/RSI, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels de la commission scolaire.

Service des ressources humaines

En matière de sécurité de l'information, le service des ressources humaines s'assure que tout employé de la commission scolaire soit avisé de la politique de sécurité de l'information et obtient son engagement au respect de la politique.

Direction de l'unité administrative

En matière de sécurité de l'information, la direction de l'unité administrative s'assure de l'application de la politique, du cadre de gestion et des directives qui en découleront. Elle est la détentrice de l'information. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de cette unité administrative.

Elle :

- voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la politique de sécurité de l'information et de tout autre élément du cadre de gestion ;

- s'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion ;

- rapporte au CSGI toute menace ou tout incident afférant à la sécurité de l'information ;

- collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'actif informationnel ;

- rapporte au CSGI tout problème lié à l'application de la politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

Utilisateur

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition dans le cadre de ses fonctions. 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. À cette fin, tout employé de la CSS 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, en signant la déclaration jointe en annexe ;

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.

8. DROIT DE REGARD ET SANCTIONS

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

La CSS a un droit de regard sur l'emploi de ses actifs informationnels par les utilisateurs, notamment par le contrôle de leurs droits d'accès à l'information. De ce fait, toute expectative de l'utilisateur en matière de protection de la vie privée s'en trouve restreinte.

Toute personne qui enfreint une règle applicable à la protection ou à la sécurité de l'information est passible notamment de l'une des sanctions suivantes :

- L'annulation des droits d'utilisation des actifs informationnels visés par la présente politique ;
- Le remboursement à la CS de toute somme que cette dernière serait dans l'obligation d'encourir à la suite d'une utilisation non autorisée, frauduleuse ou illicite des actifs informationnels visés par la présente politique ;
- Les membres du personnel s'exposent à des mesures administratives ou à des sanctions disciplinaires conformément aux conventions collectives ou aux règlements sur les conditions d'emploi des cadres ou hors cadres ainsi qu'aux lois en vigueur ;
- Les élèves s'exposent aux sanctions prévues au code de vie de l'établissement fréquenté ;

- Les partenaires, les mandataires et les fournisseurs sont passibles de mesures administratives, par exemple la résiliation du contrat ou l'expulsion de la personne qui travaille pour son compte.

Enfin, des poursuites criminelles ou pénales pourraient être entreprises contre toute personne qui enfreindrait l'une de ces règles.

Dérogation : le détenteur de l'information qui a une raison valable de ne pas se conformer à une exigence particulière ou de ne pas recourir à une mesure de sécurité déterminée peut demander une dérogation à la Direction générale après avoir pris soin d'évaluer les risques associés à cette dérogation.

9. RESPONSABLES DE L'APPLICATION

La direction générale est responsable, en collaboration avec le responsable de la sécurité de l'information (RSI), de l'application de la présente politique. Les coordonnateurs sectoriels à la gestion des incidents (CSGI) contribuent également à son application.

10. DIFFUSION

Le responsable de la sécurité de l'information (RSI), assisté du comité pour la sécurité de l'information dont fait partie au moins un coordonnateur sectoriel à la gestion des incidents (CSGI), s'assure de la diffusion et de la mise à jour de la politique.

11. ENTRÉE EN VIGUEUR

La présente politique est entrée en vigueur à la date de son adoption par le conseil des commissaires, soit le 25 juin 2019.

Jean-Philippe Bachand
Président

Édith Pelletier
Directrice générale

ANNEXE I

DÉCLARATION D'ENGAGEMENT PAR LES EMPLOYÉS QUANT AU RESPECT DES RÈGLES DE SÉCURITÉ DE L'INFORMATION

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par la commission scolaire. À cette fin, ils doivent :

- ✓ Se conformer aux directives de la commission scolaire, à la politique sur la sécurité de l'information ainsi qu'aux procédures et aux autres lignes de conduite se rapportant à la sécurité de l'information de la commission scolaire ;

- ✓ Utiliser, dans le cadre des droits d'accès qui leur sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels mis à leur disposition, en se limitant aux fins auxquelles ils sont destinés ;

- ✓ Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier la configuration des mesures de sécurité ou les désactiver ;

- ✓ Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister ;

- ✓ Signaler immédiatement à leur supérieur tout acte dont ils ont 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 ;

- ✓ Au moment de leur départ de la commission scolaire, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de l'exercice de leurs fonctions.

Je soussigné(e), _____, reconnais avoir pris connaissance des règles, ci-dessus reproduites, sur la sécurité de l'information de la commission scolaire et m'engage à les respecter.

Signature : _____ Date : _____