Commission scolaire des Grandes-Seigneuries

POLITIQUE

SÉCURITÉ DE L'INFORMATION - POLITIQUE

 # 90-01

Adoption : 10 septembre 2019

Mise en vigueur le : 11 septembre 2019

Résolution nº C.C.-4796-09-19

Autorisation

Kathlyn Morel
Directrice générale

1. CONTEXTE

Pour remplir sa mission, la Commission scolaire des Grandes-Seigneuries (CSDGS), produit, utilise, conserve ou détruit une information abondante qui concerne les citoyens, les entreprises et le personnel, ainsi que le gouvernement. Cette information peut revêtir une importance stratégique pour la CSDGS comme pour l'État et avoir une valeur légale, administrative, économique ou patrimoniale. En conséquence, l'information, c'est-à-dire l'actif informationnel, constitue une ressource essentielle qu'il convient de protéger durant tout son cycle de vie, quel qu'en soit le support ou l'emplacement.

2. OBJECTIFS

Cette politique vise une saine gouvernance de la sécurité de l'information par les objectifs suivants :

2.1 Protéger l'information tout au long de son cycle de vie, quel qu'en soit le support ou l'emplacement;

2.2 Assurer la disponibilité de l'information de façon qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée;

2.3 Assurer l'intégrité de l'information de manière que celle-ci ne soit pas détruite ni altérée de quelque façon sans autorisation et au moyen d'un support qui lui procure la stabilité et la pérennité nécessaires;

2.4 Limiter la divulgation de l'information confidentielle aux seules personnes autorisées à en prendre connaissance;

2.5 Permettre de confirmer, lorsque cela est nécessaire, l'authenticité d'un document ou l'identité d'une personne ou d'un dispositif qui accède à l'information;

2.6 Se prémunir contre le refus d'une personne de reconnaître sa responsabilité à l'égard d'un document ou d'un autre objet, notamment au regard d'un dispositif d'identification avec lequel elle a un lien;

2.7 Assurer l'archivage ou la destruction des documents en fonction de leur valeur légale, administrative, économique ou patrimoniale dans le respect du calendrier de conservation de la CSDGS et conformément aux normes en vigueur en matière de gestion documentaire.

3. CHAMP D'APPLICATION

3.1. Personnes visées

Cette politique s'applique à l'ensemble du personnel de la CSDGS, aux élèves, visiteurs, clients, mandataires, partenaires et fournisseurs ainsi qu'aux personnes qui interviennent pour leur compte. Elle concerne également l'information confiée à des tiers et toute forme d'échange ou de communication de renseignements, y compris la prestation électronique de services.

3.2. Actif informationnel

Cette politique porte sur l'actif informationnel que détient ou utilise la CSDGS, peu importe sa nature, sa localisation et le support sur lequel il se trouve, et ce, durant tout son cycle de vie, c'est-à-dire depuis sa collecte ou sa création jusqu'à sa destruction en conformité avec le calendrier de conservation de la CSDGS.

3.3. Activités

Cette politique doit être prise en considération dès la conception d'un processus ou d'un système d'information, de même qu'au moment de la préparation d'ententes, de contrats ou de conventions ou de l'acquisition d'une solution technologique.

4. PRINCIPES DIRECTEURS

4.1. Responsabilité et imputabilité

L'atteinte des objectifs de sécurité de l'information exige l'attribution claire des responsabilités à tous les échelons de l'organisation et l'adoption de processus de gestion de la sécurité assurant une reddition de comptes appropriée. Ainsi, la sécurité de l'information représente une responsabilité collective et chaque personne a l'obligation de rendre des comptes en fonction de son rôle particulier. Il s'ensuit que la sensibilisation et la formation à la sécurité de l'information s'avèrent des éléments essentiels.

Le détenteur a la responsabilité de voir au bon usage de l'information et des systèmes qui lui sont confiés. Il doit rendre compte de la mise en œuvre de mesures destinées à réduire les risques touchant la sécurité de l'information à un degré acceptable pour la CSDGS.

Dans le cas où un incident pourrait avoir un impact sur les données confidentielles relatives à la population, la CSDGS s'engage à déclarer publiquement l'événement.

4.2 Éthique

Les processus de gestion de la sécurité de l'information doivent être soutenus par une démarche d'éthique visant à assurer la régulation des conduites et à favoriser la responsabilisation individuelle.

4.3 Évolution

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être évaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques ou environnementaux ainsi que de l'évolution des menaces et des risques.

4.4 Universalité

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la limite des ressources disponibles, à des façons de faire reconnues et généralement utilisées à l'échelle nationale ou internationale.

5. RÔLES ET RESPONSABILITÉS

5.1. Conseil des commissaires

Le Conseil des commissaires :

- Adopte la politique de sécurité de l'information;
- Nomme les détenteurs de l'information qui ont la responsabilité de s'assurer de la sécurité de l'information, et des ressources qui la sous-tendent, relevant de l'autorité de leur unité administrative;
- Nomme le Responsable de la sécurité de l'information (RSI);
- Nomme les deux Coordonnateurs sectoriels de la gestion des incidents (CSGI);
- Reçoit, tous les deux ans, un plan d'action et un bilan de sécurité de l'information;
- Reçoit, annuellement, les risques de sécurité de l'information à portée gouvernementale;
- Reçoit les incidents de sécurité de l'information à portée gouvernementale lorsque ceux-ci se produisent.

5.2 Direction générale

La Direction générale :

- Détermine des mesures visant à favoriser l'application de la politique et le respect des obligations légales en matière de sécurité de l'information;
- Détermine les orientations stratégiques, les plans d'action et les bilans de sécurité de l'information;
- Détermine également les directives, les processus et les procédures qui viennent préciser ou soutenir l'application de la politique;
- Présente, au Conseil des commissaires ainsi qu'au ministère tous les deux ans, un plan d'action et un bilan de sécurité de l'information;
- Déclare annuellement, au Conseil des commissaires ainsi qu'au ministère, les risques de sécurité de l'information à portée gouvernementale;
- Déclare, au Conseil des commissaires ainsi qu'au coordonnateur organisationnel de gestion des incidents du réseau de l'éducation (COGI-réseau) du Ministère, les incidents de sécurité de l'information à portée gouvernementale lorsque ceux-ci se produisent.

5.3 Responsable de la sécurité de l'information (RSI)

Le RSI :

- Conseille la Direction générale en ce qui a trait à la détermination des orientations stratégiques et priorités d'intervention en sécurité de l'information pour la CSDGS;
- Communique ces orientations et priorités au personnel de la CSDGS;

- Assure l'arrimage de toutes les préoccupations en matière de sécurité de l'information des actifs informationnels de l'organisation et la participation des intervenants à la mise en œuvre des processus officiels de gestion;
- Veille à la coordination et à la cohérence des actions de la sécurité de l'information menées par les autres acteurs tels que les détenteurs de l'information ainsi que les unités administratives responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique;
- Met en place et anime les comités internes de coordination et de concertation en sécurité de l'information; coordonne l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information.
- Met en œuvre un processus de veille sur les menaces et vulnérabilités ainsi que sur les bonnes pratiques de sécurité de l'information en collaboration avec le Ministère et les autres RSI du réseau de l'éducation.

5.4 Coordonnateur sectoriel de la gestion des incidents (CSGI)

Le CSGI :

- Contribue à la mise en œuvre des processus officiels de la sécurité de l'information;
- Assure une veille continue sur les risques, les menaces et les vulnérabilités;
- Gère les incidents de sécurité de l'information à portée gouvernementale;
- Développe, met en place et teste le plan de réponse aux incidents de sécurité de l'information avec les membres de l'équipe de réponse aux incidents;
- Contribue aux analyses des risques en sécurité de l'information, à définir les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
- Procède à l'autoévaluation de la sécurité des actifs informationnels, notamment par des exercices d'audit de sécurité, de tests d'intrusion pour les systèmes jugés à risque ou d'exploitation des processus de gestion de la sécurité de l'information;
- Tient à jour les guides portant sur la sécurité opérationnelle des actifs informationnels et des processus.

5.5 Détenteur de l'information

Gestionnaire dans une unité administrative, le détenteur de l'information :

- A la responsabilité de l'application et du respect de la présente politique, de même que de l'application des directives touchant la sécurité de l'information et des bonnes pratiques en cette matière;
- Sensibilise chaque année les membres de son personnel à la protection de l'information, aux conséquences d'une atteinte à la sécurité de l'information ainsi qu'à leurs responsabilités en la matière.

- Assure la mise en œuvre des mesures de sécurité propres à assurer la protection de l'information stratégique ou critique qui est collectée, utilisée, communiquée, conservée ou détruite, mesures qui s'avèrent raisonnables compte tenu, notamment, de la sensibilité, de la finalité de l'utilisation, de la quantité, de la répartition et du support de l'information.
- Collabore étroitement avec le RSI et les CSGI, notamment pour la catégorisation des actifs informationnels, la détermination des exigences de sécurité, la conformité des processus, la gestion des incidents et la reddition de comptes en matière de sécurité.

5.6 Utilisateur

Tout utilisateur, y compris les employés, les élèves, les visiteurs, les mandataires, les partenaires, les fournisseurs et ceux qui agissent pour leur compte, a l'obligation de protéger l'information mise à sa disposition. L'utilisateur a notamment les responsabilités suivantes :

- S'assurer de l'intégrité et de la confidentialité de l'information de la CSDGS;
- Suivre les directives et respecter les consignes qui lui sont présentées;
- Utiliser l'information, quel que soit le support sur lequel elle se trouve, avec discernement, aux seules fins auxquelles elle est destinée et exclusivement selon les droits qui lui sont accordés;
- Assurer, le moment venu, la destruction sécuritaire des documents sensibles;
- Utiliser uniquement l'équipement et les logiciels autorisés par le Service des technologies de l'information;
- Agir avec précaution, notamment en s'abstenant d'utiliser l'information s'il a des doutes sur les règles applicables;
- Respecter les droits de propriété intellectuelle au moment de l'utilisation des produits et des documents;
- Signaler sans tarder à son supérieur immédiat toute situation ou tout incident susceptible de compromettre la sécurité de l'information.

6 DISPOSITIONS FINALES

6.1 Droit de regard et sanctions

La CSDGS 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 CSDGS 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.

6.2 Dérogation

Exceptionnellement, la Direction générale peut autoriser un détenteur de l'information à déroger à une exigence particulière ou une mesure de sécurité déterminée de la présente politique si ce dernier fait la démonstration que la situation le requiert. Toute autorisation de dérogation sera consignée dans la reddition de comptes présentée au Conseil des commissaires lors du bilan de sécurité.

6.3 Entrée en vigueur

La présente politique entre en vigueur le lendemain du jour de son adoption par le Conseil des commissaires.

ANNEXE 1 – 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 CSDGS, dans le but d'en déterminer le niveau de protection, eu égard aux risques potentiels au chapitre de la disponibilité, de l'intégrité, de la confidentialité, de l'authentification et de l'irrévocabilité (DICAI).

La CSDGS 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 CSDGS.

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.

Éthique
L'éthique fait référence à des valeurs partagées pour guider les actions. Elle implique une appropriation de règles déontologiques. Dans une situation donnée, la personne se fonde sur ces valeurs pour former son jugement et prendre une décision. Elle est amenée à réfléchir aux conséquences de ses actes avant de les poser. L'éthique fait ainsi appel au jugement de la personne et vise une action préventive.

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

À moins d'obtenir le consentement de la personne concernée, tout renseignement personnel doit être maintenu confidentiel.

De plus, l'article 23 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 : « Un organisme public ne peut communiquer le secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle, sans son consentement ».

Risque touchant la sécurité de l'information à portée gouvernementale
Ce type de risque porte atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur leur droit fondamental à la

protection des renseignements qui les concernent, sur le respect de leur vie privée, sur l'image du gouvernement ou sur la prestation de services des autres organismes publics.

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.

ANNEXE 2 – CADRE LÉGAL ET ADMINISTRATIF

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03, art. 20).

Directive sur la sécurité de l'information gouvernementale (décret 7-2014 du 15 janvier 2014).

Loi concernant le cadre juridique des technologies de l'information (RLRQ, chapitre C 1.1).

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1).

Loi sur l'administration publique (RLRQ, chapitre A-6.01).

Loi sur le vérificateur général (RLRQ, chapitre V-5.01).

Charte canadienne des droits et libertés, partie 1 de la Loi constitutionnelle de 1982 (annexe B de la Loi de 1982 sur le Canada [1982, R.-U., chapitre 11]), art. 5 et 44.

Charte des droits et libertés de la personne (RLRQ, chapitre C-12).

Code civil du Québec (LQ, 1991, chapitre 64, art. 35 à 41).

Code criminel (LRC [1985], chapitre C-46).

Loi sur la sécurité civile (RLRQ, chapitre S-2.3).

Loi sur la fonction publique (RLRQ, chapitre F-3.1.1).

Loi sur les archives (RLRQ, chapitre A-21.1).

Loi sur le droit d'auteur (LRC [1985], chapitre C-42).

Politique de gestion des documents inactifs des organismes publics.

Loi sur l'instruction publique (LQ, chapitre I-13.3).

Politiques et règlements de la Commission scolaire des Grandes-Seigneuries.