Centre de services scolaire des Grandes-Seigneuries

Québec

POLITIQUE

POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION, À L'UTILISATION DES RESSOURCES INFORMATIONNELLES ET À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

 # 90-04

Adoption le :	12 avril 2022
Mise en vigueur le :	13 avril 2022
Résolution # :	CA-2022-04-12-127

Autorisation:

Kathlyn Morel
Directrice générale

Table des matières

1. CONTEXTE

Pour remplir sa mission, le Centre de services scolaire des Grandes-Seigneuries (CSSDGS), 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 le CSSDGS 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.

Le Centre de services scolaire doit s'assurer que les ressources informationnelles qu'il met à la disposition des élèves et du personnel en tant que support à des activités pédagogiques et administratives soient utilisées adéquatement et dans le respect de sa mission. C'est dans cet esprit que le CSSDGS encourage le développement d'une citoyenneté à l'ère du numérique positive, tant pour les élèves que pour le personnel ainsi que pour les administrateurs.

2. OBJECTIFS

Cette politique vise à établir un cadre régissant l'utilisation de l'actif informationnel du centre de services scolaire.

Elle a également pour objectifs :

- De protéger l'information tout au long de son cycle de vie, quel qu'en soit le support ou l'emplacement;
- D'assurer la disponibilité de l'information de façon qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée;
- D'assurer l'intégrité de l'information de manière que celle-ci soit conservée à l'aide d'un support qui lui procure la stabilité et la pérennité nécessaire, tout en assurant que celle-ci ne soit pas détruite ni altérée de quelque façon sans autorisation;
- De sensibiliser toutes les personnes visées aux responsabilités qui leur incombent en matière de sécurité de l'information et aux impacts et conséquences que peuvent avoir leur utilisation des actifs informationnels du centre de services scolaire;
- D'assurer la gestion documentaire en fonction de la valeur légale, administrative, économique ou patrimoniale des documents, dans le respect du calendrier de conservation du CSSDGS et conformément aux normes applicables;
- D'assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et de la communication;
- De 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;
- De protéger les investissements collectifs et les utilisateurs contre un usage abusif et illégal des ressources informationnelles;
- De définir les rôles et responsabilités de chacun.
- De protéger et préserver la réputation et l'image du gouvernement, du centre de services scolaire, de ses élèves, employés et représentants en limitant la divulgation de l'information confidentielle aux seules personnes autorisées à en prendre connaissance;

3. ENCADREMENT LÉGAL ET ADMINISTRATIF

La politique trouve son fondement dans les lois ci-après énumérées :

- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
- Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives (Projet de loi numéro 95, 2021, chapitre 22);
- 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 modernisant des dispositions législatives en matière de protection des renseignements personnels (Projet de loi numéro 64, 2021, chapitre 25);
- Loi sur le vérificateur général (RLRQ, chapitre V-5.01);
- Charte des droits et libertés de la personne (RLRQ, chapitre C-12);
- Code civil du Québec (LQ, 1991, chapitre 64);
- 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);
- Loi sur l'instruction publique (LQ, chapitre I-13.3).

Elle tient également compte du cadre règlementaire applicable par le biais des documents suivants :

- Directive sur la sécurité de l'information gouvernementale (décret 7-2014 du 15 janvier 2014);
- Règlement de délégation de pouvoirs du CSSDGS (R. 10-01)
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (RLRQ, chapitre A-21.1, r.2).

Enfin, elle tient compte des politiques en vigueur au CSSDGS.

4. DÉFINITIONS

Actif informationnel
Ce terme désigne toute information consignée ou non dans un document que le système permet de 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 le CSSDGS, dans le but d'en déterminer le niveau de protection, eu égard aux risques au chapitre de la disponibilité, de l'intégrité, de la confidentialité, de l'authentification et de l'irrévocabilité (DICAI).

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 ou sa collecte, 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 du CSSDGS.

Gestionnaire d'un actif informationnel
Gestionnaire qui, au sein du centre de services scolaire, est propriétaire de données ou d'informations ou d'un système d'informations.

Identité numérique
L'identité numérique d'une personne est constituée de l'ensemble de ses codes d'accès et de ses coordonnées servant à l'identifier sur Internet. Elle se compose d'éléments d'authentification (numéro d'identification, adresse IP, adresse courriel, nom d'usager, mot de passe, nom, prénom, etc.), de données (personnelles, administratives, bancaires, professionnelles, sociales, etc.) et de signes de reconnaissance (photo d'identité, logo professionnel, etc.).

Intégrité
Propriété associée aux données qui, pendant leur traitement, leur conservation en mémoire ou leur transport par voie électronique, ne subissent aucune altération ou destruction volontaire ou accidentelle.

Citoyenneté à l'ère du numérique
La citoyenneté à l'ère du numérique réfère à une utilisation responsable des outils technologiques et environnements numériques au moment d'apprendre, de travailler, de s'informer, de collaborer, de communiquer, de créer, de se divertir, de produire et de partager des contenus.
Pour être un bon citoyen numérique, l'adoption d'habitudes et de comportements respectueux de la nétiquette, du bien-être et de la santé en ligne, de la cybersécurité, des lois, règlements et encadrements en vigueur sont essentiels. Aussi, cette citoyenneté ne peut s'exercer sans esprit critique. Elle vise à améliorer les communautés virtuelles et à stimuler l'engagement des citoyens.

Sources :
Citoyenneté à l'ère du numérique – Portrait et recommandations – Publication - Google Documents
www.citoyennetenumeriquequebec.ca
Les fondements de la littératie numérique
Continuum de développement de la compétence numérique (gouv.qc.ca)
Digital Citizenship in Schools
Citoyenneté numérique | Définir la Frontière - McGill University
http://www.slideshare.net/annecollier/making-the-case-for-digital-citizenship-111104

Nétiquette
Ensemble des conventions de bienséance régissant le comportement des internautes, notamment lors des échanges dans les forums, par courrier électronique et dans les réseaux

sociaux. (référence : Le grand dictionnaire terminologique – Office de la langue française).

Renseignements personnels
Les renseignements qui concernent une personne physique et permettent, directement ou indirectement, de l'identifier. Les renseignements personnels sont confidentiels, sauf si la personne concernée consent à leur divulgation.

Utilisateur
Toute personne qui fait usage d'un actif informationnel du centre de services scolaire.

5. PRINCIPES DIRECTEURS

5.1 Responsabilité et imputabilité

La sécurité de l'information représente une responsabilité collective et chaque personne visée par la politique doit être sensibilisée et formée en continue en matière de sécurité de l'information et a l'obligation de rendre des comptes en fonction de son rôle particulier; conséquemment, 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 assurant une reddition de comptes adéquate.

5.2 Éthique

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

5.3 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.

5.4 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.

6. CHAMP D'APPLICATION

La présente politique s'applique à tout actif informationnel que détient ou utilise le CSSDGS, 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 du CSSDGS.

De façon plus précise, cette politique doit être prise en considération dès la conception d'un processus ou d'un système d'information et dès l'ajout d'un nouveau service. De plus, elle doit être prise en compte lors de la préparation d'ententes, de contrats ou de conventions aux fins de l'acquisition d'une solution technologique.

De ce fait, toutes les personnes ci-après énumérées sont assujetties à la politique, en tout

temps et en tout lieu :

- Les employés, les élèves, les bénévoles, tous les membres de comités et autres représentants du CSSDGS;
- Les visiteurs, les clients, les mandataires, les partenaires et les fournisseurs du CSSDGS et toutes les personnes qui interviennent pour leur compte;
- Toute personne ayant un accès légitime à un actif informationnel du CSSDGS, et ce, quelle que soit la nature du lien qui l'unit au CSSDGS.

7. RÔLES ET RESPONSABILITÉS

7.1 Conseil administration

- Adopte la présente politique;
- Approuve la structure administrative permettant de nommer les gestionnaires d'un actif informationnel 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);
- Est informé et reçoit, annuellement, un plan d'action et un bilan de sécurité de l'information;
- Est informé, annuellement, des risques de sécurité de l'information à portée gouvernementale;
- Est informé des incidents de sécurité de l'information à portée gouvernementale et de leurs suivis lorsque ceux-ci se produisent.

7.2 Comité de vérification

- Est consulté lors de la révision de la politique;
- Prend acte, annuellement, du bilan de sécurité de l'information et de son plan d'action;
- Au besoin, transmet ses recommandations au conseil d'administration.

7.3 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;
- Met en place le comité sur l'accès à l'information et la protection des renseignements personnels et en est responsable;
- Approuve le plan et le bilan annuel 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 CA ainsi qu'au ministère tous les deux ans, un plan d'action et un bilan de sécurité de l'information;
- Déclare annuellement, au CA ainsi qu'au ministère, les risques de sécurité de l'information à portée gouvernementale;
- Déclare, au CA 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.

- Dans le cas où un incident pourrait avoir un impact sur les données confidentielles relatives à la population, le CSSDGS s'engage à déclarer publiquement l'événement;
- Peut autoriser la direction du service des technologies de l'information à procéder à une vérification des informations personnelles d'un utilisateur ou de l'utilisation des ressources informationnelles par celui-ci, si elle a des raisons de croire que son utilisation contrevient à la politique ou aux lois et règlements en vigueur.
- Exceptionnellement, la Direction générale peut autoriser un gestionnaire d'un actif informationnel à déroger à une exigence particulière ou à une mesure de sécurité découlant 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 incluse au bilan de sécurité de l'information présentée au conseil d'administration.

7.4 Direction du service des technologies de l'information

- Instaure des mesures de contrôle et sécurité appropriées pour protéger adéquatement l'actif informationnel;
- Est responsable de la gestion des actifs informationnels et à ce titre, autorise l'aliénation, la modification ou la destruction de tout ou partie de celui-ci;
- Reçoit et analyse l'information contenues aux registres de transactions sur l'utilisation des actifs informationnels et peut utiliser cette information pour détecter les activités non autorisées, illicites ou illégales;
- Avec l'autorisation de la direction générale, et s'il a des raisons de croire que l'utilisateur contrevient à la politique ou aux lois et règlements en vigueur, procède à la vérification des informations personnelles d'un utilisateur ou de l'utilisation par celui-ci, des ressources informationnelles;
- Applique la présente politique;
- Assure la gestion des incidents relatif à la sécurité de l'information;
- Assure la réalisation du bilan annuel ainsi que de l'audit externe.

7.5 Responsable de la sécurité de l'information (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 CSSDGS;
- Communique ces orientations et priorités au personnel de la CSSDGS;
- 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 cohérence et à la coordination des actions relatives à la sécurité de l'information menées par les autres acteurs tels que les gestionnaires d'un actif informationnel ainsi que les unités administratives responsables des ressources informationnelles, de la gestion documentaire, de l'accès à l'information et de la protection des renseignements personnels
- 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 de formation continue et de sensibilisation en matière de sécurité de l'information, destiné au personnel;
- 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;
- Participe, à la demande de la direction générale, au comité sur l'accès à l'information

et la protection des renseignements personnels.

7.6 Coordonnateur sectoriel de la gestion des incidents (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.

7.7 Gestionnaire d'un actif informationnel

Gestionnaire dans une unité administrative, le gestionnaire d'un actif informationnel :

- 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.
- Voit 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 le CSSDGS.
- Applique les mesures de contrôle et de sécurité développées par le STI.

Dans le cas où le gestionnaire d'un actif informationnel est la direction d'un établissement, les rôles et responsabilités suivants lui sont aussi attribués :

- Exceptionnellement, peut autoriser la direction du service des technologies de l'information à procéder à une vérification de l'utilisation des ressources informationnelles faite par un élève, si elle a des motifs sérieux de croire que cette utilisation contrevient à la politique ou aux lois et règlements en vigueur. Pour ce faire, elle doit fournir au STI les informations nécessaires pour procéder à la demande, et ce, selon le guide d'accompagnement de gestion des comportements non désirés en ligne. La vérification doit être strictement et directement liée au(x) motif(s) identifié(s);
- S'assurer que les codes de vie des établissements intègrent :
  - Un code de conduite relatif à l'utilisation des actifs informationnels qui respecte la présente politique;

- Une mention à l'effet que l'utilisation des ressources informationnelles par un élève peut faire l'objet de vérification à la demande de la direction de l'établissement.

7.8 Utilisateur

- Prendre les mesures requises pour protéger l'information mise à sa disposition, notamment en assurant la confidentialité des codes d'accès et mots de passe utilisés;
- S'assurer de l'intégrité et de la confidentialité de l'information du CSSDGS;
- 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, selon le calendrier de conservation, la destruction sécuritaire des documents sensibles;
- Utiliser uniquement l'équipement et les logiciels autorisés par le Service des technologies de l'information;
- Utiliser l'équipement et les logiciels uniquement à des fins autorisées, légales et légitimes;
- Respecter l'intégrité des actifs informatiques et informationnels auxquels il a accès;
- Agir avec précaution, notamment en s'abstenant d'utiliser l'information s'il a des doutes sur les règles applicables;
- Adopter un langage et un comportement respectueux de la mission du centre de services scolaires, en vue de s'assurer d'en préserver la réputation;
- Respecter les droits de propriété intellectuelle au moment de l'utilisation des produits et des documents;
- Signaler sans tarder au Service des Technologies de l'Information toute situation ou tout incident susceptible de compromettre la sécurité de l'information.
- Respecter les droits d'auteur, entre autres s'abstenir d'utiliser des reproductions illicite s de logiciels et de données ou de participer directement ou indirectement à une telle reproduction;
- Respecter la confidentialité des informations contenues dans les équipements informatiques ou de télécommunication;

8. UTILISATION DES RESSOURCES INFORMATIONNELLES

L'utilisation des actifs informationnels du CSSDGS est un privilège qui peut être modifié ou révoqué en tout temps pour tout utilisateur qui ne se conforme pas à la Politique.

Les actifs informationnels doivent être utilisés prioritairement pour la réalisation des activités liées à la réalisation de la mission du CSSDGS. L'utilisation à des fins personnelles d'un ordinateur, d'une tablette et d'un téléphone par les élèves et employés est tolérée, pour autant qu'elle n'entrave pas l'exécution des fonctions professionnelles (ex : utilisation au détriment de ses tâches, aussi appelé « vol de temps ») ou la réalisation des objectifs pédagogiques (ex : stocker sur son ordinateur professionnel du contenu à caractère violent accessible aux élèves) et qu'elle se fait dans le respect de la présente politique (ex : utiliser les actifs informationnels dans le cadre d'un deuxième emploi de courtier en placements).

Tout accès ou tentative d'accès non autorisé aux actifs informationnels du Centre de services scolaire constitue une violation de la présente politique.

En tout temps, l'utilisateur doit respecter les termes et conditions d'utilisation des logiciels, applications, sites et services en ligne, incluant les médias sociaux. De plus, toute utilisation à des fins commerciales, illicites, frauduleuses, diffamatoires, discriminatoires ou qui incite au racisme, au sectarisme, à la haine ou à la violence est strictement interdite.

Sauf en cas d'urgence et pour des raisons techniques, une vérification qui nécessiterait la lecture des informations personnelles et privées d'un utilisateur ne peut être effectuée que par des personnes autorisées, dans le cadre de leurs fonctions, après avoir donné, à la personne concernée, l'opportunité de préserver
ces informations et avoir obtenu son accord.

Tout actif informationnel contenant des données confidentielles doit être protégé, au minimum, par un processus d'accès nécessitant un mécanisme d'identification et d'authentification de l'utilisateur. Cet accès doit être limité aux personnes autorisées seulement, en fonction de la nature de l'information et des applications utilisées.

Tout accès ou tentative d'accès non autorisé aux actifs informationnels du Centre de services scolaire constitue une violation de la présente politique.

9. CONFIDENTIALITÉ DES INFORMATIONS

L'information contenue dans les actifs informationnels du centre de services scolaires est confidentielle si elle a le caractère d'un renseignement personnel ou d'un renseignement que le centre de services scolaire peut ou doit protéger en vertu d'une loi, d'un règlement, d'un contrat ou d'une entente de confidentialité.

Le Centre de services scolaire doit publier sur son site Internet les règles encadrant sa gouvernance à l'égard des renseignements personnels approuvées par son comité sur l'accès à l'information et la protection des renseignements personnels.

Il est interdit de divulguer à une personne non autorisée, toute information confiée à l'organisation ou obtenue à l'occasion de l'exercice d'une fonction confidentielle.

Lorsque le Centre de services scolaire a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel, il a la responsabilité de prendre toute mesure appropriée en lien avec celui-ci.

L'utilisateur doit s'abstenir de dévoiler ou laisser prendre connaissance de tout document, message ou information sous quelque forme que ce soit sans avoir été préalablement autorisé par son supérieur ou par le responsable de l'accès aux documents désigné en vertu de la *Loi de l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

Le centre de services scolaire ne peut garantir la confidentialité de toutes les communications se retrouvant sur les ressources informationnelles du centre de services scolaire. L'utilisateur doit présumer que toute communication qu'il crée, envoie, reçoit ou archive sur les systèmes électroniques du centre de services scolaire peut être lue et entendue par quelqu'un d'autre que le destinataire.

10. DROIT D'AUTEUR

En tout temps, l'utilisateur doit respecter les droits d'auteur et les autres droits de propriété intellectuelle des tiers.

Les reproductions de logiciels, de banques de données et informations (textuelles, sonores, symboliques ou visuelles) ne sont autorisées qu'à des fins de copies de sauvegarde ou selon les termes de la licence d'utilisation qui les régit.

Personne ne doit utiliser, effectuer ou participer à la reproduction de logiciels, d'objets numérisés ou de leur documentation sans le consentement du propriétaire des droits d'auteur.

11. DROIT DE REGARD ET SANCTIONS

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 :

- La restriction de ses droits d'utilisation des actifs informationnels visés par la présente politique;
- Le remboursement au CSSDGS de toute somme que ce dernier 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;
- Dans le cas des membres du personnel, 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;
- Dans le cas des élèves, les sanctions sont prévues au code de vie de l'établissement fréquenté;
- Pour les partenaires mandataires ou les fournisseurs, les contrats en vigueur peuvent être résiliés et des dommages et intérêts pourraient leur être réclamés. De plus, les personnes qui travaillent pour ceux-ci peuvent se voir expulser des lieux de travail du CSSDGS.

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

12. Processus et procédures

Gestion des incidents

Le CSSDGS possède un processus de la gestion des incidents qui 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 du CSSDGS, dont le plan local des mesures d'urgence.

Les incidents touchant la sécurité de l'information à portée gouvernementale sont gérés à travers le processus de déclaration des incidents majeurs. Ce type d'incident 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.

Gestion des accès et des mots de passes
Ultimement, la gestion des accès et des mots de passes est encadrée par une procédure spécifique afin de déterminer quelles sont les règles à suivre afin de se conformer aux normes en vigueur et aux facilités d'usage.

Gestion de l'utilisation des services infonuagiques
Ultimement, l'utilisation des services infonuagiques est encadrée par une procédure spécifique et a pour objectif d'établir les conditions dans lesquelles les utilisateurs peuvent faire usage de plateforme infonuagique tel que Office365, iCloud, Google Drive, Dropbox ou autres, mais aussi de conserver l'aspect du respect de la langue française par ces types d'outils lorsque vient le moment d'en faire le choix.

13. MÉCANISME DE RÉVISION ET DE VÉRIFICATION

Le service des technologies de l'information procède annuellement à un audit en sécurité de l'information via une firme externe et présente dans son bilan annuel une synthèse du rapport. Si, à la suite des recommandations contenues dans ce rapport, il émerge des modifications à apporter, une révision de la politique sera adoptée par le conseil d'administration. Enfin, le service des technologies de l'information procède aussi à l'évaluation de la politique aux deux ans et au besoin, il soumet à la direction générale les éléments à modifier. Toute modification à la politique doit être adoptée par le conseil d'administration.

14. DISPOSITIONS FINALES

Le conseil d'administration adopte la présente politique qui annule et remplace toute autre politique ou règle antérieure portant sur le même sujet et entre en vigueur le lendemain du jour de son adoption par le conseil d'administration.