Centre de services scolaire des Grandes-Seigneuries
Québec

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 :	13 avril 2022
Modification le :	25 juin 2025
Mise en vigueur le :	26 juin 2025
Résolution # :	CA-2025-06-25-382

Autorisation :

Christian Duval
Directeur général par intérim

Table des matières

1. CONTEXTE

Pour remplir sa mission, le Centre de services scolaire des Grandes-Seigneuries (ci-après le « 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 constitue une ressource essentielle qu'il convient de protéger durant tout son cycle de vie, quel qu'en soit le support ou l'emplacement.

L'application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03), de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) et de la Directive gouvernementale sur la sécurité de l'information (2021) du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics, imposent des obligations importantes aux établissements scolaires ainsi qu'à leurs partenaires en matière de sécurité de l'information.

Pour se conformer à ses obligations réglementaires et légales ainsi que pour atteindre des standards de sécurité de l'information élevés, le CSSDGS a l'obligation d'adopter, de garder à jour et de veiller à l'application d'une politique de sécurité de l'information et d'un encadrement relatif à la protection des renseignements personnels. Cette politique a pour objectif d'encadrer la gestion des risques, la gestion des accès aux ressources informationnelles, la gestion des événements, la gestion de la continuité des activités ainsi que tout processus disposant d'un lien avec la sécurité de l'information.

Les modalités précises d'application de la politique seront encadrées par des procédures qui viendront en soutenir l'application et qui seront adoptées par la direction générale dans le respect du Règlement de délégation de fonctions et de pouvoirs du CSSDGS.

2. OBJECTIFS

Cette politique vise à doter le CSSDGS d'un cadre général de gestion des ressources informationnelles en vue d'assurer la sécurité de l'information et la protection des renseignements personnels. 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.
- Préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou de la divulguer à des personnes, entités ou processus non autorisés.
- De sensibiliser toutes les personnes visées aux responsabilités qui leur incombent en matière de sécurité de l'information et de protection des renseignements personnels et aux impacts et conséquences que peuvent avoir leurs utilisations des ressources informationnelles du CSSDGS.
- 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 CSSDGS, de ses élèves, employés et représentants en limitant la divulgation de l'information confidentielle aux seules personnes autorisées à en prendre connaissance.

3. ENCADREMENT

La présente politique découle des lois ci-après énumérées :

- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (ci-après le « LAI ») (RLRQ, chapitre G-1.03)
- 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 le vérificateur général (RLRQ, chapitre V-5.01)
- Charte des droits et libertés de la personne (RLRQ, chapitre C-12)
- Code civil du Québec (RLRQ, 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 (RLRQ, chapitre I-13.3)

De plus, la présente politique s'appuie notamment sur le cadre réglementaire, de même que l'ensemble des politiques, directives, règles, arrêtés, normes et pratiques gouvernementales applicables.

Enfin, la présente politique doit être lue en concordance avec les orientations, encadrements ou autres outils en vigueur au CSSDGS concernant la sécurité de l'information et la protection des renseignements personnels.

4. DÉFINITIONS

Actifs informationnels

Ensemble des informations ayant une valeur pour l'organisation qui en est détentrice et dont la gestion doit être assurée de manière stratégique, notamment par la mise en place d'un système de classement, de mesures de sécurité particulières et d'un cycle de vie préétabli.

Modèle de classification de sécurité des données numériques

Le modèle de classification de sécurité des données numériques gouvernementales permet aux organismes publics de classifier les données numériques gouvernementales qu'ils détiennent afin de leur accorder un niveau de sécurisation adéquat. L'objectif est de déterminer le niveau de protection, eu égard aux risques au chapitre de la disponibilité, de l'intégrité, de la confidentialité

Cycle de vie de l'information

L'ensemble des étapes que parcourt une information, de 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.

Incident de confidentialité

L'accès, l'utilisation et la communication non autorisés par la loi d'un renseignement personnel, ainsi que la perte de ce renseignement ou toute autre atteinte à sa protection

Événement de sécurité

Toute forme d'atteinte, présente ou appréhendée, telle une cyberattaque ou une menace à la confidentialité, à l'intégrité à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité du CSSDGS.

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.

Renseignement personnel

Renseignement qui concerne une personne physique et permet directement ou indirectement de l'identifier.

Responsable d'un actif informationnel

Personne qui, au sein du CSSDGS, est responsable de la gouvernance des données ou de l'information ou d'un système d'information.

Ressources informationnelles

Ensemble des ressources utilisées par une organisation, dans le cadre de ses activités de gestion de l'information, pour l'accomplissement de sa mission, pour la prise de décision ou pour la résolution de problèmes.

Les ressources informationnelles incluent notamment les ressources humaines, matérielles, financières ou technologiques directement affectées à l'acquisition, au développement, à l'entretien, à l'exploitation, au traitement, à la circulation, à l'utilisation, à la protection, à la conservation et à la destruction des éléments d'information. Une personne, un fichier ou un système informatique, par exemple, peut faire partie des ressources informationnelles d'une organisation.

Risques liés à la sécurité de l'information

Tout événement lors du traitement, de l'utilisation ou de l'entreposage comportant un degré d'incertitude, qui pourrait porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information et causer un préjudice.

Utilisateur

Toute personne qui fait usage d'une ressource informationnelle du CSSDGS.

5. CHAMP D'APPLICATION

Personnes visées

La présente politique s'adresse aux utilisateurs de l'information ou des ressources informationnelles du CSSDGS.

Elle s'applique à toute personne qui est au service ou qui utilise ou qui est membres des instances et des comités du CSSDGS, qu'elle travaille dans ses locaux ou à distance. Elle s'applique également à toute personne liée par contrat, par entente ou par prêt de service ainsi qu'à toute personne employée par un fournisseur du CSSDGS dans l'accomplissement de son mandat.

Actifs visés

L'information visée est celle que le CSSDGS, ou un tiers pour son compte, détient ou utilise dans l'exercice de ses fonctions, et ce, quel que soit le support de conservation, de traitement ou de transmission.

Activités visées

Cette politique concerne l'ensemble des activités entrant dans le cycle de vie de l'information à savoir : la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation et la destruction des actifs informationnels du CSSDGS, en tout lieu, en tout temps et sur tout support.

6. CONTENU

6.1 PRINCIPES DIRECTEURS

a) 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 continu 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 et de protection des renseignements personnels exige l'attribution claire des responsabilités à tous les échelons de l'organisation et l'adoption de processus assurant une reddition de comptes adéquate.

b) Éthique

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

c) Évolution

Les pratiques et les solutions retenues en matière de sécurité de l'information et de protection des renseignements personnels 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.

d) Universalité

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

6.2 RÔLES ET RESPONSABILITÉS

a) Conseil d'administration (ci-après le «CA »)

- Adopte la présente politique et ses révisions le cas échéant.
- Nomme le chef de la sécurité de l'information organisationnelle (ci-après le « CSIO »), sur recommandation de la direction générale.
- Nomme les deux coordonnateurs organisationnels des mesures de sécurité de l'information (ci-après le « COMSI »), sur recommandation de la direction générale.
- Est informé des événements de sécurité de l'information à portée gouvernementale et de leurs suivis lorsque ceux-ci se produisent.

b) Comité de vérification

- Est consulté lors de la révision de la politique.
- Prend acte de l'audit portant sur le respect des obligations en matière de sécurité de l'information découlant de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (ci-après le « LGGRI »).
- Au besoin, transmet ses recommandations au conseil d'administration.
- Est informé et reçoit annuellement les orientations stratégiques des plans d'action, des audits et des redditions de comptes en matière de sécurité de l'information;

c) 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 et de protection des renseignements personnels.

- Met en place le comité sur l'accès à l'information et la protection des renseignements personnels et en est responsable.
- Détermine les procédures et les processus qui viennent préciser ou soutenir l'application de la politique.
- Prend acte des orientations stratégiques, des évaluations des risques, des plans d'action, des audits et des redditions de comptes en matière de sécurité de l'information.
- Assume le processus de désignation des personnes agissant à titre de CSIO, de COMSI et formule ses recommandations au CA.
- Exerce ou délègue par écrit les fonctions de responsable de la protection des renseignements personnel.
- Prend acte de l'audit portant sur le respect des obligations en matière de sécurité de l'information découlant de la LGGRI.
- Déclare annuellement, au CA, les risques de sécurité de l'information à portée gouvernementale.
- Déclare au CA les évènements de sécurité de l'information à portée gouvernementale et les informent des suivis lorsque ceux-ci se produisent.
- Autorise, le cas échéant, 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 autorise un responsable 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 est consignée au registre constitué à cette fin.

d) Responsable de l'accès à l'information et de la protection des renseignements personnels

- Reçoit les demandes d'accès aux documents, de communication ou de rectification de renseignement personnel, s'assure qu'elles soient traitées selon les dispositions de la LAI, incluant la transmission de tout avis requis par la LAI et rend une décision dans le délai prévu.
- Prête assistance au requérant lorsque sa demande n'est pas suffisamment précise ou lorsqu'il le requiert, pour identifier le document susceptible de contenir les renseignements recherchés.
- Prête assistance au requérant qui le demande pour l'aider à comprendre la décision transmise.
- Veille à ce que tout document qui a fait l'objet d'une demande d'accès, de communication ou de rectification soit conservé le temps requis pour permettre au requérant d'épuiser les recours prévus à la LAI.
- Veille à l'analyse et prends position sur l'application d'une situation d'exception prévue à la LAI en matière de collecte, d'utilisation, de communication ou de conservation des renseignements personnels.
- S'assure de la mise en place et de la tenue des différents registres prévus dans la LAI.
- Veille à établir et tenir à jour le plan de classification des documents que le CSSDGS détient.
- Traite les plaintes relatives à la protection des renseignements personnels.
- Assure un rôle de soutien et de conseil relativement à toute question touchant l'accès aux documents ou la protection des renseignements personnels.

e) Chef de la sécurité de l'information organisationnelle

- Mets en œuvre les décisions prises par le chef gouvernemental de la sécurité de l'information (ci-après le « CGSI ») et son chef délégué de la sécurité de l'information (ci-après le « CDSI »).
- Est responsable de la mise en œuvre des indications et directives concernant la sécurité de l'information.

- Contribue à la mise en œuvre du cadre de gouvernance de la sécurité de l'information au sein du CSSDGS.
- Assure l'intégration des exigences de sécurité de l'information lors de la réalisation de projets de développement, d'acquisition, d'évolution ou de remplacement d'une ressource informationnelle.
- Notifie de façon immédiate le CDSI lorsqu'un événement de sécurité présente un risque qu'un préjudice sérieux soit causé.
- Assure la gestion des actions nécessaires en cas d'événement de sécurité.
- Assure la tenue du registre des événements de sécurité.
- Assure le lien et transmets l'information requise par les CGSI et CDSI.
- Met en place au sein de son organisation les comités et les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination.
- Coordonne le développement des compétences en sécurité de l'information pour l'ensemble du personnel.

f) Comité sur l'accès à l'information et la protection des renseignements personnels

- Soutient le CSSDGS dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la Loi sur l'accès à l'information et sur la protection des renseignements personnels.
- Est consulté au début de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
- Suggère, à toute étape d'un projet des mesures de protection des renseignements personnels applicables à ce projet.
- Est consulté avant la publication des règles de confidentialité ou de sa modification.
- Veille à la sensibilisation et à la formation des employés ou mandataires du CSSDGS en matière de protection des renseignements personnels.
- Exerce toute autre fonction en lien avec la protection de renseignements personnels à la demande de la direction générale.

g) Coordonnateur organisationnel des mesures de sécurité de l'information

Le COMSI agit sur le plan opérationnel. Il intervient dans la mise en œuvre des mesures et il soutient le CSIO du CSSDGS, notamment en matière de la gestion des événements et des risques en sécurité de l'information.

Il collabore aussi avec le CSIO du CSSDGS à l'élaboration de stratégies en sécurité de l'information afin de :

- Maintenir le registre des événements liés à la sécurité de l'information.
- Effectuer et participer aux analyses de risques en sécurité de l'information.
- Gérer le processus de gestion de déclaration des événements de sécurité et de résolution de problèmes et contribuer à sa mise en place.
- S'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux processus de gestion des menaces, des vulnérabilités et des incidents.
- Contribuer au processus formel de gestion des droits d'accès aux ressources informationnels.
- Intervenir dans la mise en œuvre des mesures de sécurité de l'information, tel que précisé dans les mesures gouvernementales.
- Soutenir le CSIO notamment pour la gestion des risques relatifs à la sécurité de l'information et la gestion des événements de sécurité.
- Représenter le CSSDGS auprès du Réseau d'alerte gouvernemental.

h) Direction du service des technologies de l'information

- Est responsable de l'application de la présente politique.
- Veille à l'intégration des exigences de sécurité dans l'utilisation quotidienne des ressources informationnelles.
- Identifie, en collaboration avec le CSIO, les mesures de protection pour sécuriser les actifs informationnels en fonction de leur sensibilité et dans le respect des exigences législatives, réglementaires et contractuelles.
- Instaure des mesures de contrôle et sécurité appropriées pour protéger adéquatement les ressources informationnelles.
- 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.
- Peut recevoir et analyser l'information contenue 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.
- Assure la gestion des événements relatifs à la sécurité de l'information.
- Assure la réalisation du bilan de sécurité de l'information ainsi que de l'audit externe.

i) Responsable d'actifs informationnels

Employé responsable d'un actif informationnel dans une unité administrative :

- S'assure 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 du 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.
- Veille à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous sa responsabilité.
- Participe à la catégorisation des actifs informationnels sous sa responsabilité et à l'analyse de risques.
- Veille à la protection des actifs informationnels en conformité avec la politique de sécurité de l'information.
- Au besoin, collabore à la mise en œuvre de toute mesure pour améliorer la sécurité de l'information afin de remédier à un événement de sécurité ou à un incident de confidentialité.

j) Direction d'unité administrative

- S'assure du respect de la présente politique par les employés ou mandataires du CSSDGS sous sa responsabilité.
- Identifie, pour son unité administrative, les renseignements personnels qu'il détient.
- Identifie les catégories d'employés ou mandataires du CSSDGS sous sa responsabilité qui ont accès aux renseignements personnels, ainsi que les catégories de renseignements personnels qui leur sont accessibles.
- Met en place dans son établissement ou service des mesures de protection des renseignements personnels qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité, de leur utilisation, de leur quantité, de leur répartition et de leur support, voit à leur diffusion et à leur application par les employés ou mandataires sous leur responsabilité.

- En collaboration avec le Comité sur l'accès à l'information et la protection des renseignements personnels, veille à ce que les formations et les activités de sensibilisation prévues au présent cadre de référence soient offertes aux employés ou mandataires sous leur responsabilité et s'assurer que ces derniers y participent.

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

- Exceptionnellement, autorise 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.
- Le cas échéant, s'assure que les codes de vie des établissements intègrent : un code de conduite relatif à l'utilisation des ressources informationnelles qui respecte la présente politique.
- Une mention selon laquelle l'utilisation des ressources informationnelles par un élève peut faire l'objet de vérification à la demande de la direction de l'établissement.

k) Utilisateur

La responsabilité de la sécurité de l'information et de la protection des renseignements personnels incombe à tous les utilisateurs d'actifs informationnels. L'utilisateur qui collecte, utilise, communique ou détruit une information en est responsable et il doit donc contribuer à sa protection.

À cette fin, l'utilisateur :

- Respecte la présente politique et tout autre encadrement du CSSDGS en matière de sécurité de l'information et d'utilisation des actifs informationnels et de protection des renseignements personnels.
- Utilise uniquement l'équipement et les logiciels autorisés par le service des technologies de l'information.
- Respecte l'intégrité des ressources informationnelles auxquels il a accès.
- S'assure de protéger l'intégrité et de la confidentialité de l'information du CSSDGS.
- Est responsable des actions résultant de l'usage de son identifiant, de son code d'accès ou de son mot de passe et prend les mesures requises pour en assurer la protection et la confidentialité.
- Avise son supérieur immédiat, de toute situation ou événement susceptible de compromettre la sécurité d'information ou la protection des renseignements personnels.
- Au besoin, participe à la catégorisation des actifs informationnels de son service.
- Utilise les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre approprié à son utilisation et aux fins auxquelles ils sont destinés.
- Accède uniquement aux renseignements personnels qui sont nécessaires à l'exercice de ses fonctions.
- Respecte les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver.
- Participe aux formations et aux activités de sensibilisation en matière de sécurité de l'information et de protection des renseignements personnels.
- Collabore, sur demande, à toute intervention relative à une menace à la sécurité de l'information ou à la protection des renseignements personnels.
- Signale 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 sur CSSDGS.

6.3 UTILISATION DES RESSOURCES INFORMATIONNELLES

L'utilisation des ressources informationnelles 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 ressources informationnelles doivent être utilisées 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 ressources informationnelles dans le cadre d'un deuxième emploi de courtier en placements).

Tout accès ou tentative d'accès non autorisé aux ressources informationnelles du CSSDGS 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 ressources informationnelles du CSSDGS constitue une violation de la présente politique.

6.4 CONFIDENTIALITÉ DES INFORMATIONS

L'information contenue dans les ressources informationnelles du CSSDGS est confidentielle si elle a le caractère d'un renseignement personnel ou d'un renseignement que le CSSDGS peut ou doit protéger en vertu d'une loi, d'un règlement, d'un contrat ou d'une entente de confidentialité.

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 CSSDGS 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 LAI.

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

6.5 DROIT DE REGARD ET SANCTIONS

Le CSSDGS exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des ressources informationnelles, et ce, dans le respect de la vie privée des utilisateurs. 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 ressources informationnelles visées par la présente politique.
- Le remboursement de toute somme que le CSSDGS serait dans l'obligation d'encourir à la suite d'une utilisation non autorisée, frauduleuse ou illicite des ressources informationnelles visées 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.
- 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.

7. MÉCANISME DE RÉVISION

La direction du service des technologies de l'information procède à l'évaluation de la politique aux deux ans et au besoin, soumet à la direction générale les éléments à modifier. Toute modification à la politique doit être adoptée par le conseil d'administration.

8. 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.

9. LEXIQUE

CA	Conseil d'administration
CDSI	Chef délégué de la sécurité de l'information
CGSI	Chef gouvernemental de la sécurité de l'information
COMSI	Coordonnateur organisationnel des mesures en sécurité de l'information
CSIO	Chef de la sécurité de l'information organisationnelle
LAI	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
L.R.C.	Lois refondues du Canada
L.R.Q.	Lois refondues du Québec
RLRQ	Recueil des lois et des règlements du Québec