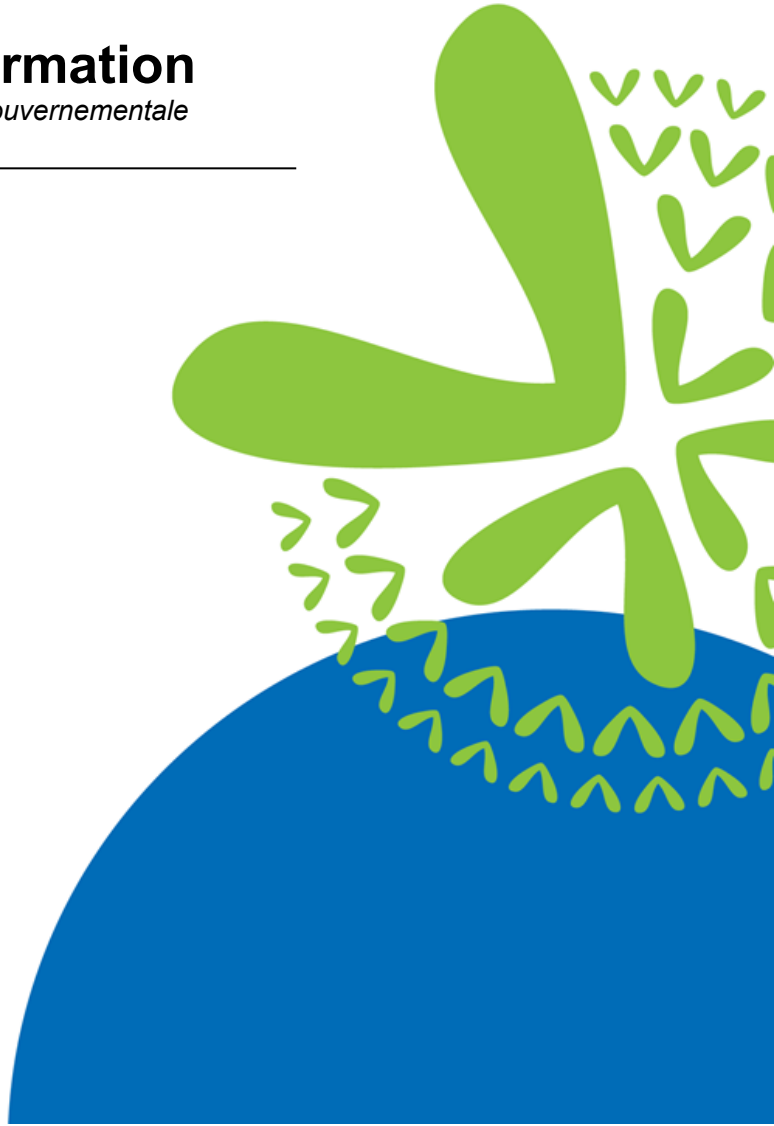
Centre
de services scolaire
des Samares
Québec

Politique de sécurité de l'information

En fonction de la *Directive sur la sécurité de l'information gouvernementale*

Service des technologies de l'information



Adoption : **CA 2024-03-26-069**

Table des matières

1. Contexte

L'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI) (LRQ, Loi 133) et de la *Directive sur la sécurité de l'information gouvernementale* (DSIG) (directive du Conseil du trésor du Québec applicable aux centres de services scolaires) crée des obligations aux établissements scolaires en leur qualité d'organismes publics.

Ainsi, la DSIG oblige les centres de services scolaires à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de sécurité de l'information – dont les principales modalités sont définies dans la DSIG – en ayant recours, notamment, à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents. Ceci demande que deux (2) rôles soient comblés au sein de chaque centre de services scolaire. Tel qu'il est stipulé dans le Guide de nomination, un Chef de la sécurité de l'information organisationnelle (CSIO) et deux (2) Coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI) doivent être désignés.

Cette politique permet au Centre de services scolaire des Samares (CSSS) d'accomplir ses missions, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'il a créée ou reçue et dont il 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, son intégrité ou sa 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 du CSSS et du gouvernement.

2. Cadre légal et administratif

La présente politique s'inscrit dans un contexte régi par les législations provinciale et fédérale, et en conformité avec les normes reconnues en la matière, soit notamment :

- la *Charte des droits et libertés de la personne* (RLRQ, c. C-12);
- la *Loi sur l'instruction publique* (LRQ, c. I-13.3);
- le *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (A-21.1, r. 2);
- le *Code civil du Québec* (LQ, 1991, c. 64);
- la *Loi sur l'administration publique* (LRQ, c. A-6.01);
- la *Loi sur la fonction publique* (LRQ, c. F-3.1.1);
- la *Loi canadienne sur les droits de la personne* (LRC, 1985, c. H-6);
- 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, c. G-1.03);
- la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1);
- le *Code criminel* (LRC, 1985, c. C-46);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (A-2.1, r. 2);
- la *Directive sur la sécurité de l'information gouvernementale*;
- la *Loi sur le droit d'auteur* (LRC, 1985, c. C-42);
- la *Loi sur les archives* (LRQ, c. A-21.1);
- la *Politique de gestion des documents et de l'information* du CSSS;
- la *Politique sur la gestion des actifs informatiques* du CSSS;
- la *Politique d'utilisation des ressources informatiques* du CSSS.

3. Objectifs

La présente politique a pour objectif d'affirmer l'engagement du CSSS 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, le CSSS doit veiller à la mise en place des mécanismes, règles et procédure visant à assurer :

- 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, le CSSS 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 du CSSS.

4. Champ d'application

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à tout le personnel, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'élève ou de public utilise les actifs informationnels du CSSS ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que le CSSS 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.

La présente politique étant fondée sur l'obligation gouvernementale d'assurer globalement la sécurité de l'information, ses dispositions doivent être appliquées strictement. Aucune disposition du cadre de gestion du CSSS ne peut y contrevenir ou y déroger. Le cadre de gestion du CSSS doit en tout temps veiller à respecter les règles établies par la présente politique. S'il y a lieu, les adaptations nécessaires doivent être apportées.

5. Principes directeurs

5.1. Protection de l'information

a) Le CSSS adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale;

b) Le CSSS reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, qu'ils doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection dont les actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ils sont exposés;

c) La sécurité des actifs informationnels est soutenue par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

5.2. Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée.

Sont notamment considérés comme confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

5.3. Sensibilisation et formation

Le CSSS s'engage, sur une base régulière, à sensibiliser et à 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.

5.4. Droit de regard

Le CSSS exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels.

6. Obligations des intervenants clés en matière de sécurité de l'information

La présente politique fixe les obligations en matière de sécurité de l'information attribuées, notamment au dirigeant de l'organisme, au chef organisationnel de la sécurité de l'information, aux détenteurs, aux gestionnaires d'entités administratives et aux utilisateurs.

a) Le dirigeant de l'organisme : il est le premier responsable de la sécurité de l'information relevant de son autorité.

b) Le chef de la sécurité de l'information organisationnelle : il assiste le dirigeant de l'organisme dans la détermination des orientations stratégiques et des priorités d'intervention.

c) Le détenteur de l'information : employé désigné par le CSSS, appartenant à la classe d'emploi de niveau cadre et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

d) Les gestionnaires : ils sont chargés de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité.

e) Les utilisateurs : ils doivent se conformer aux directives gouvernementales, à la présente politique et aux règles qui leur sont applicables, en signant la déclaration d'engagement jointe en annexe.

Les rôles et les responsabilités attribuées à d'autres intervenants ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information sont définis dans le cadre de gestion de la sécurité de l'information, en complément à la présente politique.

7. Obligation des utilisateurs

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le CSSS. À cette fin, il doit :

a) prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer, 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 du CSSS;

f) au moment de son départ du CSSS, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de l'exercice de ses fonctions.

8. Sanctions

Tout utilisateur des actifs informationnels du CSSS qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l'information qui en découlent ou aux dispositions prévues dans le cadre de gestion s'expose à des mesures disciplinaires, administratives ou légales, selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles disciplinaires internes applicables (dont celles des conventions collectives de travail et des Règlements du CSSS). Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

Le CSSS peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

9. Dispositions finales

a) Le conseil d'administration approuve la présente politique.

b) La présente politique entre en vigueur au moment de son adoption.

c) Le chef de la sécurité de l'information organisationnelle est chargé de la mise en œuvre des dispositions de la présente politique et de ses directives d'applications.

d) La présente politique doit être révisée à l'occasion de changements qui pourraient l'affecter.

e) La présente politique sert de complément au cadre de gestion de la sécurité de l'information. Les obligations qui en découlent sont précisées dans des directives.

Centre
de services scolaire
des Samares
Québec

ANNEXE I – Définitions

Actif informationnel : L'ensemble des documents, tels que définis à l'article 3 de la *Loi concernant le cadre juridique des technologies de l'information*, constitués d'information portée par un support, produit ou reçu par tout employé du CSSS dans l'exercice de ses fonctions.

Sont assimilés au document numérique 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, un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le CSSS qui peut être accessible avec un dispositif des technologies de l'information (logiciels, progiciels, didacticiels, banque d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Y est également assimilée toute information stockée dans un format numérique sur un de ces médias : disque, base de données, clé USB, mémoire flash, vidéo, photo numérique, ordinateur portable, ordinateur de table, tablettes, téléphone intelligent, etc.

Sont assimilées au document non numérique toute information autre que numérique, accessible par un dispositif plus traditionnel tel une filière ou un classeur ou fixée sur un support analogique, dont le papier, le microfilm, la pellicule, la photo papier, etc. Un tel document peut se retrouver sur un mur.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées, concernées et autorisées et de n'être divulguée qu'à celles-ci.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

Document : Ensemble constitué d'information portée par un support. L'information y est délimitée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles. [...] est assimilée au 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.

Source : Loi concernant le cadre juridique des technologies de l'information - article 3

Guide : Document administratif à caractère pédagogique qui vise à faciliter l'application des prescriptions d'une politique, d'une directive ou éventuellement d'une norme, sans en avoir le caractère contraignant.

Source : Grand dictionnaire terminologique

Intégrité : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Mesure de sécurité de l'information : Moyen concret assurant, partiellement ou totalement, la protection d'un actif informationnel contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

Source : OQLF – Grand dictionnaire terminologique

Norme : Accord entériné par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi.

Source : Lexique gouvernemental

Procédure : Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche.

Source : OQLF – Grand dictionnaire terminologique

Processus : Suite cohérente d'activités et d'opérations d'une organisation traduisant les besoins de la clientèle et des employés dans une logique de création de valeur.

Renseignement personnel : Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de sécurité.

Source : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

Ressources informationnelles : Les actifs informationnels ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

Standard : Norme qui n'a été ni définie ni entérinée par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., mais qui s'est imposée par la force des choses, parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'entreprises ou encore d'un consortium.

Utilisatrice ou utilisateur : Toute personne de l'organisation de quelque catégorie d'emploi, de statut d'employé, tout élève ainsi que toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel de l'organisation ou y a accès.

Centre
de services scolaire
des Samares
Québec

ANNEXE II – Déclaration d'engagement par les utilisateurs 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 le Centre de services scolaire des Samares (CSSS). À cette fin, ils doivent :

- se conformer aux directives gouvernementales, à la politique sur la sécurité de l'information ainsi qu'aux directives sectorielles, aux procédures et aux autres lignes de conduite se rapportant la sécurité de l'information du CSSS;

- 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 du ministère;

- au moment de leur départ du CSSS, 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 du CSSS et m'engage à les respecter.

Signature : _____ **Date :** _____