Centre
de services scolaire
de la Capitale
Québec

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

ϖ ϖ ϖ ϖ ϖ

Service :	Services de l'informatique
Code d'identification :	P.SI.02
Numéro de résolution :	CA : 34/01/21
Date d'entrée en vigueur :	20 janvier 2021

TABLE DES MATIÈRES

1.0 TITRE

Politique sur la sécurité de l'information

2.0 ÉNONCÉ

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) créent des obligations aux établissements scolaires en leur qualité d'organismes publics quant à l'adoption, la mise en œuvre, au maintien et à l'application d'une politique sur la sécurité de l'information.

Cette politique permet au centre de services scolaire de la Capitale (CSSC) d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue et dont elle est le gardien. Cette information liée à la clientèle, aux ressources humaines, matérielles, technologiques et financières est accessible sur des formats numériques et non numériques, dont les risques d'atteinte à sa disponibilité, intégrité ou confidentialité peuvent avoir des conséquences liées à :

- La vie, la santé ou le bien-être des personnes;
- L'atteinte à la protection des renseignements personnels et à la vie privée;
- La prestation de services à la population;
- L'image du CSSC et du gouvernement

La DSIG définit les principales modalités de la politique en ayant recours, notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion des incidents et la gestion de l'accès à l'information.

3.0 FONDEMENTS

La politique de sécurité s'inscrit principalement dans un contexte régi par :

- La *Charte des droits et libertés de la personne* (LRQ, chapitre C-12);
- La *Loi sur l'instruction publique* (LRQ, c. c. I-13.3);
- *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (LRQ c. A-21.1, r.1);
- Le *Code civil du Québec* (LQ, 1991, chapitre 64);
- La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, Loi 133);
- La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1);
- Le *Code criminel* (LRC, 1985, chapitre C-46);

- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, r. 2);
- La *Directive sur la sécurité de l'information gouvernementale*;
- La *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- *Politique d'utilisation des technologies de l'information du CSSC (PUTI)*;
- *Code éthique et de déontologie applicable aux employés et aux intervenants de la commission scolaire de la Capitale*.

4.0 OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du CSSC à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information. Plus précisément, il veille à :

- La disponibilité de l'information aux personnes autorisées;
- L'intégrité de l'information;
- La confidentialité de l'information.

De plus, le CSSC désigne, tel que le stipule le *Guide de nomination*, un responsable de la sécurité de l'information (RSI) et deux coordonnateurs sectoriels de la gestion des incidents (CSGI).

5.0 DÉFINITIONS

Actif informationnel
Une information, quel que soit son canal de communication (téléphone analogique ou numérique, télégraphe, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation. Exemples : Disque dur, clé USB, dossiers papiers dans un classeur, boîte de documents au secteur des archives, etc. (Guide d'élaboration d'une politique de sécurité de l'information – p. 9)

Catégorisation
La catégorisation de l'information est le processus d'assignation d'une valeur à certaines caractéristiques d'une information. Cette catégorisation qualifie le degré de sensibilité en termes de disponibilité, d'intégrité et de confidentialité et, par conséquent, le niveau adéquat de protection à lui accorder.

Confidentialité
La confidentialité d'une information est la propriété d'une information accessible uniquement aux personnes ou entités désignées et autorisées, et ne pouvant être divulguée qu'à celles-ci.

Cycle de vie de l'information
L'ensemble des étapes que franchit l'information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation du CSSC.

Détenteur de l'information
Le détenteur de l'information est un membre du personnel d'encadrement qui a la responsabilité d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels du CSSC.

Directives locales concernant la sécurité informationnelle
L'ensemble des règles, des consignes, des procédures et des bonnes pratiques reconnues qui encadrent les activités en matière de sécurité informationnelle des unités administratives du CSSC.

Document
Un document est un ensemble d'informations délimitées et structurées de façon tangible ou logique sur un support adapté, intelligible sous forme de mots, de sons ou d'images.

Disponibilité
La disponibilité d'une information est la propriété d'une information accessible en temps voulu et de la manière requise à une personne autorisée.

Incident
Un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information. Un incident nécessitera une intervention concertée sur le plan gouvernemental lorsqu'il peut avoir des conséquences liées à la vie et la santé ou le bien-être des personnes, à l'atteinte à la protection des renseignements personnels et à la vie privée, à la prestation de services à la population ou à l'image du CSSC et du gouvernement.

Information
Un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Intégrité
L'intégrité d'une information est la propriété d'une information ne subissant aucune altération ni destruction sans autorisation ou de façon erronée, et qui est conservée sur un support et préservée avec des moyens lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Mesure de sécurité de l'information
Un moyen concret assurant partiellement ou totalement la protection de l'information du CSSC 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.

Renseignement personnel
Une information concernant une personne physique et qui 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 la sécurité de l'information.

Risque de sécurité de l'information
Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de service à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection de leurs renseignements personnels et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de service fournie par d'autres organismes publics**.**

Sécurité de l'information
La protection de l'information et des systèmes d'information contre les risques et les incidents.

Système d'information
L'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

Technologie de l'information
Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

Utilisateur
Tout élève, employé ou personne physique autorisée qui accède par l'entremise des réseaux numérique et non numérique aux actifs informationnels du CSSC dans l'accomplissement de sa mission. Les membres de son personnel ainsi que les élèves sont les premiers utilisateurs de ces actifs informationnels.

6.0 CHAMPS D'APPLICATION

Les **personnes visées** par la présente politique sont tous les employés du CSSC, et elle s'étend également à toute personne dument autorisée (bénévoles, partenaires, consultants fournisseurs, etc.) qui utilise ou qui accède à des actifs informationnels du CSSC. À cette fin, il doit :

- Prendre connaissance de la présente politique, des directives locales concernant la sécurité informationnelle, de la PUTI et de toutes autres lignes de conduite se rapportant à la sécurité de l'information du CSSC;
- 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;
- Respecter les mesures de sécurité mises en place sur tous les équipements, systèmes d'information, applications ou autres environnements contenant des données sensibles tout en évitant la modification de leur configuration ou de leur désactivation;
- 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 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 CSSC.

Les personnes visées ainsi que les élèves ont l'obligation de protéger les actifs informationnels détenus et mis à leur disposition par le CSSC dans le respect de la PUTI.

7.0 PRINCIPES GÉNÉRAUX

Les principes directeurs qui guident les actions du CSSC en matière de sécurité de l'information sont les suivants :

- S'assurer de bien connaître l'information à protéger, en identifier les détenteurs de l'information et leurs caractéristiques de sécurité;
- Reconnaître l'importance de la *Politique de sécurité de l'information*;
- Reconnaître que l'environnement technologique des actifs informationnels est en changement constant et interconnecté avec le monde;
- Protéger l'information tout au long de son cycle de vie;
- S'assurer que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;
- S'assurer que l'utilisation des actifs informationnels par les utilisateurs soit encadrée par la *Politique de sécurité de l'information* et soutenue par des directives locales précisant ce qui est permis et ce qui ne l'est pas.

8.0 GESTION DES RISQUES

La gestion des risques s'inscrit dans un processus qui s'amorce par une analyse de risques rigoureuse. Cette analyse doit permettre de connaître la valeur de l'information à protéger (dossier professionnel d'un élève, relevé d'impôt en formation FP, dossier santé d'un employé, ordre du jour des rencontres du CA du CSS, statistiques de réussite, appels d'offres, dossiers des contribuables, intranet du CSSC). La catégorisation des actifs informationnels à jour soutient cette analyse en qualifiant la valeur de ces informations à protéger.

L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de protection à mettre en œuvre pour leur déploiement dans l'environnement du CSSC. Le niveau de protection de l'information est établi en fonction :

- De la nature de l'information et de son importance;
- Des probabilités d'accident, d'erreur ou de malveillance auxquelles elles sont exposées;
- Des conséquences de la matérialisation de ces risques;
- Du niveau de risque acceptable par le CSSC.

La gestion des risques liés à la sécurité de l'information numérique et non numérique se doit de respecter les recommandations et les obligations provenant du gouvernement,

notamment lorsque les risques sont à portée gouvernementale, ils devront être déclarés conformément à la Directive sur la sécurité de l'information gouvernementale (DSIG).

9.0 GESTION DES INCIDENTS

Le CSSC déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires à l'obtention des buts suivants :

- Limiter l'occurrence des incidents en matière de sécurité de l'information;
- Gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Le processus de gestion des incidents liés à la sécurité de l'information numérique et non numérique recommandée par les autorités gouvernementales se doit d'être respecté, en mettant en place les modalités suivantes de :

- Prévention
- Détection
- Réaction
- Rétablissement
- Suivi

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés au ministère de l'Éducation conformément à la DSIG. Dans la gestion des incidents, le CSSC peut exercer ses pouvoirs et ses prérogatives en égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

10.0 DIRECTIVES

La responsabilité des directives est dévolue aux services suivants :

UNITÉS ADMINISTRATIVES ⇨ / DIRECTIVES ⇩	Service de l'informatique	Secrétariat général	Autres services	Écoles et Centres
Gestion des accès	☒	☒	☒	☒
Gestion des vulnérabilités	☒			
Gestion des copies de sauvegardes	☒			
Continuité des affaires	☒			
Protection du périmètre du réseau	☒			
Utilisation d'un appareil personnel	☒			
Protection des actifs de l'information non numérique		☒	☒	☒
Protection des actifs de l'information numérique	☒	☒		☒
Gestion des fournisseurs	☒	☒	☒	☒
L'internet des objets	☒			

10.1. GESTION DES ACCÈS

Le CSSC élabore une directive sur la gestion des accès afin de protéger la disponibilité, l'intégrité et la confidentialité de l'information numérique et non numérique. Cette directive inclut l'approbation, l'attribution, la revalidation, le retrait et la journalisation de ces accès, ainsi que la conservation des historiques des événements permettant des audits ultérieurs.

10.2. GESTION DES VULNÉRABILITÉS

Le CSSC déploie des mesures pour maintenir à jour les logiciels et applications de son parc informatique afin de maintenir les vulnérabilités au niveau le plus bas possible pour diminuer les risques d'une cyberattaque.

10.3. GESTION DES COPIES DE SAUVEGARDE

Le CSSC élabore une stratégie de copie de sauvegarde pour se prémunir contre une perte de données numériques et non numériques.

10.4. CONTINUITÉ DES AFFAIRES

Le CSSC élabore une stratégie de continuité des affaires advenant qu'un incident cause l'arrêt de la prestation de service de ce dernier.

10.5. PROTECTION DU PÉRIMÈTRE DU RÉSEAU

Le CSSC instaure des mécanismes de protection et des exercices de tests d'intrusion et balayages de vulnérabilités pour identifier les points d'entrées susceptibles de donner un accès inapproprié à des individus ou des programmes malicieux.

10.6. UTILISATION D'UN APPAREIL PERSONNEL

Tous les utilisateurs d'appareils personnels sont autorisés sur le réseau sans fil public du CSSC après avoir accepté les conditions d'utilisation contenues dans sa PUTI pour s'y connecter.

10.7. PROTECTION DES ACTIFS DE L'INFORMATION NON NUMÉRIQUE ET NUMÉRIQUE

Le CSSC élabore une directive de protection des actifs de l'information non numérique et numérique traitant notamment de la protection, de la diffusion et de la disposition des actifs.

10.8. GESTION DES FOURNISSEURS

Le CSSC élabore une directive décrivant un processus de gestion de ses fournisseurs pour prévenir d'éventuels incidents, divulgations ou pertes de données ou d'introduire de virus sur son réseau.

10.9. L'INTERNET DES OBJETS

Le CSSC élabore un encadrement pour l'Internet des objets.

11.0 RÔLES ET RESPONSABILITÉS

11.1. DIRECTION GÉNÉRALE

La direction générale est le premier répondant de la sécurité de l'information en étroite collaboration avec la direction des services de l'informatique et le RSI. Elle

est responsable d'identifier les activités de gestion devant faire l'objet d'un encadrement.

11.2. RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI)

Le RSI communique à la direction générale les orientations et les priorités en matière de sécurité de l'information et s'assure de l'arrimage et de la participation de tous les intervenants du CSSC. Il est désigné par la plus haute autorité dirigeante.

11.3. COORDONNATEUR SECTORIEL DE LA GESTION DES INCIDENTS (CSGI)

Le CSGI apporte un soutien au RSI afin de s'acquitter des responsabilités édictées par la présente politique. Il est l'interlocuteur officiel auprès de l'organisme responsable de la sécurité informationnelle au ministère de l'Éducation. Il est désigné par la plus haute autorité dirigeante.

11.4. SECRÉTAIRE GÉNÉRAL

Le secrétaire général participe, avec le CSGI et le RSI, à l'identification des risques et des mesures de sécurité physique permettant de protéger les actifs informationnels non numériques du CSSC.

11.5. SERVICES DE L'INFORMATIQUE (SI)

Les Services de l'informatique s'assurent de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels ils interviennent. Les SI s'assurent également en collaboration avec les services des ressources humaines et des unités administratives concernées qu'un nouvel employé, stagiaire ou bénévole soit informé des exigences de la *Politique de sécurité de l'information* et obtiennent son engagement au respect de celle-ci. Afin d'assurer une conduite adéquate et une responsabilisation individuelle des personnes visées, des activités de sensibilisation et de formation sont offertes périodiquement par les SI.

11.6. SERVICES DES RESSOURCES MATÉRIELLES

Les services des ressources matérielles participent, avec le RSI et le CSGI, à l'identification des risques et des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du CSSC.

11.7. DÉTENTEUR DE L'INFORMATION

Le détenteur de l'information a la responsabilité d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels du CSSC en veillant à l'accessibilité, à l'utilisation et à la protection des actifs informationnels sous la responsabilité de celui-ci.

12.0 MESURES ADMINISTRATIVES OU DISCIPLINAIRES

Un manquement à la politique et aux mesures de sécurité de l'information qui en découlent peut entraîner, sur décision de l'autorité hiérarchique compétente selon la délégation de pouvoir en vigueur, et dans le respect des conventions collectives et de tout

contrat de travail, l'application de toute mesure administrative ou disciplinaire appropriée à la nature et à la gravité du manquement.

13.0 CADRE DE GESTION

Le cadre de gestion de la sécurité de l'information renforce les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins du CSSC en matière de réduction du risque associé à la protection de l'information. Il comprend :

13.1. CONSEIL D'ADMINISTRATION (CA)

Le conseil d'administration adopte la politique sur la sécurité de l'information.

13.2. COMITÉ AVISEUR SUR LA SÉCURITÉ INFORMATIONNELLE (CASI)

Ce comité est formé du RSI, CSGI, de la direction générale adjointe aux affaires administratives et du secrétaire général. Un employé en sécurité informationnelle peut se joindre sur demande au comité aviseur. Le comité aviseur a les rôles et responsabilités suivants :

Sécurité informationnelle

- D'assister le RSI à mettre en place les directives locales en matière de sécurité informationnelle pour assurer la protection du CSSC et la conformité à la réglementation;
- De mettre en places les plans d'action et les bilans de sécurité informationnelle, les activités de sensibilisation ou de formation ainsi que toute proposition d'action en matière de sécurité de l'information;
- De permettre les échanges et les discussions entre les parties prenantes sur l'évolution des projets en sécurité informationnelle.

Gestion des incidents

- De mettre en place une équipe de réponses aux incidents de sécurité numériques et non numériques;
- D'élaborer une procédure de réponses aux incidents;
- D'assurer que les contrôles sont en place pour identifier et analyser un incident;
- De s'assurer d'un processus de validation des tests aux réponses d'incidents.

Continuité des affaires

- D'analyser les processus d'affaires et identifier ceux qui auront un impact majeur au CSSC;
- De réaliser des tests de continuités des affaires pour en valider l'efficacité.

14.0 ENTRÉE EN VIGUEUR

La présente politique entre en vigueur en date du 20 janvier 2021.