RECUEIL DE GESTION		POLITIQUE	
Centre de services scolaire des Draveurs Québec		SECTEUR	
		SERVICE SECRÉTARIAT GÉNÉRAL ET DU TRANSPORT SCOLAIRE	
SUJET	POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION		
IDENTIFICATION	CODE : 50-39-01		PAGE : 1
RÉSOLUTION NO :	AMENDEMENT NO :	DATE	SIGNATURE
C490-0525		2025-05-05	Original signé par la présidence du conseil d'administration

1. RÉFÉRENCES

La *Politique sur la sécurité de l'information* s'inscrit principalement dans un contexte régi par :

- *Charte des droits et libertés de la personne* (L.R.Q. c. C-12);
- *Code civil du Québec* (L.Q., 1991, chapitre 64);
- *Code criminel* (L.R.C., 1985, chapitre C-46);
- *Loi sur l'instruction publique* (L.R.Q. c. l-13.3);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. c. A-2.1);
- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (R.L.R.Q. 2021 chapitre 25);
- *Loi sur les archives* (L.R.Q. c. A-21.1);
- *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (L.R.Q. c. A-21.1, r.1);
- *Loi sur le droit d'auteur* (L.R.C. 1985, c C-42);
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q. chapitre G-1.03);
- *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
- *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, r. 2);
- *Règlement sur les incidents de confidentialité* (chapitre A-2.1, r. 3.1);
- *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* (gouvernement du Québec – 2010);
- *Directive gouvernementale sur la sécurité de l'information* (Décret 1514-2021 du 8 décembre 2021);

-
- *Politique gouvernementale de cybersécurité* (SCT, mars 2020).
- Conventions collectives en vigueur au Centre de services scolaire des Draveurs

De plus, le CSSD a adopté les règlements, politiques et directives suivantes :

- *Politique les communications électroniques et leur usage* (50-23-01).

2. PRÉAMBULE

En tant qu'organisme public, le Centre de services scolaire des Draveurs (ci-après le CSSD) reconnaît que l'information et les technologies qui la supportent sont essentielles à ses opérations courantes et à l'accomplissement de sa mission, et vu la valeur administrative, légale et financière de ses actifs informationnels, ils doivent faire l'objet d'une évaluation continue, d'une utilisation et d'une protection appropriées et adéquates tout au long de leur cycle de vie, selon les bonnes pratiques en matière de sécurité informationnelle et avec une approche de gestion des risques, 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*, de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, et de la *Directive gouvernementale sur la sécurité de l'information* du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics, impose des obligations importantes au CSSD.

Pour se conformer et répondre à ses obligations réglementaires et légales, le CSSD doit adopter, garder à jour et veiller à l'application d'une *Politique sur la sécurité de l'information* pour assurer la mise en place des processus formels de celle-ci afin d'encadrer la gestion des risques, la gestion des accès aux actifs informationnels, la gestion des incidents et la gestion de la continuité des activités.

3. CHAMP D'APPLICATION

La politique vise sans exception l'ensemble des personnes physiques et morales, régulières ou occasionnelles, peu importe son statut, appelé à utiliser les actifs informationnels du CSSD citant entre autres :

- Le personnel à l'emploi du CSSD;
- Les élèves du CSSD;
- Les partenaires, fournisseurs, contractants et tiers du CSSD.

La politique vise aussi toutes informations et actifs informationnels :

- Appartenant au CSSD;
- Détenu par un tiers, mais appartenant au CSSD;
- Utilisés et détenus par un tiers au bénéfice ou au nom du CSSD;
- Et ce quel que soit le support de conservation électronique, technologique ou papier.

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 CSSD que ce soient dans le périmètre de ses locaux, dans un autre endroit physique ou à distance.

4. DÉFINITIONS

Actif informationnel : désigne une information, quel que soit son support (papier, microfilm, clé USB, disque dur, espace infonuagique, etc.) ou son canal de communication (courriel, téléphone, réseau informatique, etc.) un système ou une technologie de l'information ou un ensemble de ces éléments.

Autorisation : attribution par une autorité de droits d'accès aux actifs informationnels qui consiste en un privilège d'accès accordé à une personne, à un dispositif ou à une entité.

Cadre de gestion : l'ensemble de consignes que sont les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues qui encadrent les activités d'un établissement tel que le CSSD.

Code d'accès : mécanisme d'identification et d'authentification par un code individuel et un mot de passe ou de ce qui en tient lieu, notamment une carte magnétique, ou carte à puce, servant à identifier de façon unique un utilisateur qui utilise un actif informationnel du CSSD.

Confidentialité : propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées.

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

Disponibilité : propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

Équipement informatique : ordinateurs, mini-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communications, de réception et de traitement de l'information, et tout équipement de télécommunications.

Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiées, ni altérées, ni détruites sans autorisation.

Plan de relève informatique : ensemble de procédures qui décrivent de façon précise les mesures à suivre pour remettre en état de fonctionnement un système informatique à la suite d'une panne ou d'un sinistre majeur.

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

Technologies de l'information : regroupent les techniques principalement de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie) qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre de l'information.

5. ÉNONCÉ DES PRINCIPES GÉNÉRAUX

Protection de l'information

Disponibilité

La disponibilité garantit que les utilisateurs autorisés d'un système ont un accès opportun et ininterrompu aux informations contenues dans ce système, ainsi qu'au réseau. Les informations doivent être accessibles en temps utile et de la manière requise par un utilisateur autorisé. Afin d'aider à assurer cette disponibilité, des mesures de contrôles doivent être mises en place.

Intégrité

L'intégrité des données consiste à garantir que les données n'ont pas été modifiées d'aucune façon au cours de leur communication, qu'il s'agisse de données au repos, en transit ou en mémoire. Afin d'assurer l'intégrité des données, des mesures de sécurité physiques et d'accès logique doivent être mises en place.

Confidentialité

La confidentialité vise à empêcher tout accès non autorisé à des informations sensibles. Elle a pour but de s'assurer qu'une information, une donnée, soit accessible uniquement par les personnes autorisées. La confidentialité de l'information doit aussi être assurée tout au long de son cycle de vie. Afin de garantir la confidentialité, des mesures de contrôles doivent être mises en place.

Catégorisation de l'information

L'information constitue une ressource essentielle qui doit être protégée tout au long de son cycle de vie, raison pour laquelle il est primordial de garder à jour l'inventaire de l'ensemble des actifs informationnels de l'organisation. L'un des premiers intrants de la sécurité de l'information est la connaissance de la sensibilité de l'information des actifs informationnels d'une organisation. La catégorisation des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des actifs dans le but d'en déterminer le niveau de protection.

Il est important de réévaluer la catégorisation des actifs informationnels sur une base périodique pour s'assurer que la catégorisation attribuée est toujours appropriée en fonction des modifications des obligations légales et contractuelles, ainsi que des changements dans l'utilisation des données ou leur valeur pour le CSSD. Cette évaluation devrait être effectuée par le détenteur de l'actif.

6. OBJECTIFS

La présente Politique constitue le cadre général qui vise la gestion des actifs informationnels dans le respect des droits et obligations du CSSD en cette matière. Elle pourra garantir et répondre aux objectifs de sécurité de l'information et plus spécifiquement pour :

- Assurer la protection de l'actif informationnel tout au long de son cycle de vie, quel que soit le support ou l'emplacement;
- Assurer l'intégrité de l'information en la préservant contre toute destruction, modification et altérations de quelques façons sans autorisation;
- Assurer la disponibilité de l'information pour qu'elle soit accessible au moment voulu et utilisable à la demande de l'entité autorisée;
- Préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou divulguée à des personnes, entités ou processus non autorisés;
- Regrouper les lignes directrices, les rôles et responsabilités des intervenants en sécurité;
- Identifier et classifier les actifs informationnels du CSSD selon leurs degrés de criticité et veiller constamment à leur évaluation ainsi que leur protection adéquate;
- Assurer la conformité aux lois et cadres réglementaires;
- Mettre en place un plan de continuité des activités et de relève informatique;
- Assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements personnels.

7. RÔLES ET RESPONSABILITÉS

Conseil d'administration

- Le conseil d'administration adopte la présente politique ainsi que toute modification.

Direction générale

- La direction générale, en tant que premier responsable de la sécurité de l'information, entérine le plan d'action et les mesures proposées par le comité de sécurité. Elle assume aussi le processus de délégation des rôles de chef de la sécurité de l'information organisationnelle (CSIO) et du coordonnateur organisationnel des mesures de sécurité de l'information (COMSI).

Chef de la sécurité de l'information organisationnelle (CSIO)

La personne assumant la fonction de CSIO est un membre du personnel d'encadrement d'un organisme public. Celui-ci assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. La fonction de CSIO est déléguée par la direction générale.

Le CSIO est responsable de la diffusion et de la mise en application de la politique.

À titre de responsable de l'application de la présente politique, il doit :

- Conseiller la direction générale du CSSD en ce qui a trait à la détermination des orientations stratégiques et des priorités en matière de sécurité de l'information;

- Assurer l'arrimage de toutes les préoccupations en matière de sécurité de l'information;
- Communiquer au conseil d'administration, à la demande de la direction générale, les orientations et les priorités d'intervention gouvernementales en matière de sécurité;
- S'assurer de la participation du CSSD à la mise en œuvre des processus officiels de gestion de la sécurité de l'information;
- Assurer la coordination et la cohérence des actions de sécurité de l'information menées au sein du CSSD par d'autres acteurs, tels que les détenteurs de l'informations ainsi que les unités responsables des actifs informationnels, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique;
- Coordonner et s'assurer de la mise en œuvre des processus officiels de sécurité de l'information au sein du CSSD permettant, notamment, d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Comité sur la sécurité de l'information

Ce comité est composé des personnes suivantes :

- CSIO;
- COMSI;
- COMSI délégué;
- Secrétaire général;
- Responsable de la protection des renseignements personnels.

Sur demande du comité, des personnes employées peuvent être invitées pour apporter leur soutien et expertise aux membres du comité.

Le comité a les rôles et responsabilités suivants :

Sécurité informationnelle

- Assister le CSIO à mettre en place les directives locales en matière de sécurité informationnelle pour assurer la protection du CSSD et la conformité à la réglementation;
- Mettre en place les plans d'actions et les bilans de sécurité informationnelle, les activités de sensibilisation ou de formation ainsi que toute proposition d'actions en matière de sécurité de l'information;
- Permettre les échanges et les discussions entre les parties prenantes sur l'évolution des projets en sécurité informationnelle.

Gestion des incidents

- Mettre en place une équipe de réponses aux incidents de sécurité numériques et non numériques;
- Élaborer une procédure de réponses aux incidents;
- Assurer que les contrôles sont en place pour identifier et analyser un incident;

- Assurer un processus de validation des tests aux réponses d'incidents.

Continuité des affaires

- Analyser les processus d'affaires et identifier ceux qui auront un impact majeur au CSSD;
- Réaliser des tests de continuité des affaires pour en valider l'efficacité.

Coordonnateur organisation des mesures de sécurité de l'information (COMSI)

Le COMSI agit sur le plan opérationnel. Il intervient dans la mise en œuvre des mesures et apporte le soutien nécessaire au CSIO de l'établissement, notamment en matière de la gestion des incidents et des risques en sécurité de l'information.

Le COMSI représente l'organisme public auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) au CSSD, en soutien au CSIO.

Il collabore auprès du CSIO du CSSD à l'élaboration des divers éléments stratégiques et tactiques en sécurité de l'information. Pour ce faire, il doit :

- Maintien le registre des événements et des incidents liés à la sécurité de l'information;
- Effectue et participe aux analyses de risques de sécurité de l'information;
- Gère le processus de gestion, de déclaration des incidents et de résolution de problème et contribue à sa mise en place;
- Contribue au processus formel de gestion des droits d'accès à l'information.

Direction du Service des technologies de l'information (STI)

Le STI s'assure 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 développements ou d'acquisition des systèmes d'information dans lesquels il intervient. Pour ce faire, il doit :

- Participer activement à l'analyse de risque, à l'évaluation des besoins et des mesures à mettre en œuvre, et à l'anticipation de toute menace en matière de sécurité des systèmes informatiques;
- Appliquer des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, tel que l'interruption ou la révocation temporaire – lorsque les circonstances l'exigent – des accès aux utilisateurs ou des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause;
- Participer, avec le Service du secrétariat général et du transport scolaire, à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique.

Service du secrétariat général et du transport scolaire

Le Service du secrétariat général et du transport scolaire veille à la conservation de l'information détenues par le CSSD. Il met en place et voit à l'application des règles en matière de protection, d'utilisation, d'accessibilités et de conservation des actifs informationnels. Il effectue les enquêtes nécessaires, avec le STI, lors de contraventions réelles ou apparentes à la présente politique.

Il s'assure que les ententes de services et les contrats conclus avec des fournisseurs, des partenaires, des consultants et des organismes externes sont conformes aux exigences en matière de sécurité de l'information.

Responsable de la protection des renseignements personnels

La personne responsable de la protection des renseignements personnels veille à assurer le respect et la mise en œuvre de la Loi sur l'accès à l'information et la protection des renseignements personnels et afin de mettre en œuvre des politiques et pratiques encadrant la gouvernance des renseignements personnels.

Service des ressources humaines

Le service des ressources humaines s'assure que tout nouvel employé du CSSD soit informé de la présente politique et obtient son engagement au respect de celle-ci.

Service des ressources matérielles

Le Service des ressources matérielles participe à l'identification des mesures de sécurité physique, incluant l'accès aux équipements, permettant de protéger adéquatement les actifs informationnels du CSSD. Il participe également à la mise en place et aux recommandations des correctifs permettant d'assurer cette sécurité.

Responsable d'actifs informationnels (détenteur)

La personne responsable d'actifs informationnels est la personne cadre détenant l'autorité au sein d'un service ou d'une école, qu'elle soit d'ordre pédagogique ou d'ordre administratif, et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il ou elle :

- Participe à la catégorisation de l'information de l'unité sous sa responsabilité et à l'analyse de risques;
- Veille à la protection de l'information et des systèmes d'information en conformité avec la *Politique de sécurité de l'information*;
- Rapporte tout événement ou toute menace liée à la sécurité de l'information;
- Collabore à la mise en œuvre de toute mesure pour améliorer la sécurité de l'information afin de remédier à un incident au besoin.

Utilisatrices et utilisateurs

La responsabilité de la sécurité de l'information du CSSD incombe à toutes les utilisatrices et à tous les utilisateurs des actifs informationnels. L'utilisatrice ou l'utilisateur qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à la protéger.

À cette fin, l'utilisatrice ou l'utilisateur doit :

- Se conformer à la présente politique et à toute autre directive du CSSD en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- Être responsable des actions résultat de l'usage de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers, à moins qu'il démontre que les actions posées par un tiers ne découlent pas d'une négligence ou d'une malveillance de sa part;
- Aviser une personne responsable, une personne enseignante ou son supérieur immédiat, de toute situation susceptible de compromettre la sécurité de l'actif informationnel;
- Au besoin, participer à la catégorisation de l'information de son service;
- Utiliser 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;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- Collaborer à toute intervention visant à indiquer ou à mitiger une menace ou un incident à la sécurité de l'information.

8. CADRE DE GESTION

La mise en œuvre de la présente politique s'appuie sur la définition d'un cadre de gestion en sécurité de l'information qui précise le champ d'action des différents intervenants. Le cadre de gestion précise l'organisation fonctionnelle en matière de sécurité de l'information et rend possibles la définition d'objectifs clairs et une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information sont réévaluées de manière périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces et des risques.

La politique de sécurité de l'information du CSSD se base sur cinq axes fondamentaux de gestion, comme suit.

Gestion des identités et des accès (GIA)

La gestion des accès est encadrée et contrôle pour faire en sorte que l'accès, la divulgation et l'utilisation de toute information détenue par le CSSD soient strictement réservés aux personnes autorisées pour protéger la confidentialité.

Gestion des vulnérabilités

La gestion des vulnérabilités se caractérise par un déploiement des mesures pour maintenir à jour les logiciels du parc informatique afin de garder les vulnérabilités au niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une gestion de notifications des vulnérabilités venant des fournisseurs ou des prestataires de services doit être en place pour qu'elles soient évaluées et corrigées le cas échéant.

Gestion du risque

La gestion du risque touchant l'actif informationnel du CSSD est basée sur une analyse des menaces encourues reliées à l'intégrité, la disponibilité et la confidentialité de l'information détenue par le CSSD. De cette analyse découlent des directives reliées à l'utilisation et l'opération des systèmes d'information ainsi qu'aux résultats escomptés.

Gestion des incidents

La gestion des incidents se caractérise par la mise en place de procédures de compte rendu, d'analyse relativement aux incidents de sécurités et de mesures correctives pour y donner suite. Les mesures déployées visent à assurer la continuité des services. Dans la gestion des incidents, le CSSD peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'actif informationnel.

Gestion de la reprise et de la continuité des affaires

La gestion de la reprise et de la continuité des affaires se caractérise par la mise en place des processus pour identifier les incidents opérationnels majeurs susceptibles de menacer le CSSD telles les catastrophes naturelles, les pannes d'électricité ou de télécommunication, les pannes informatiques, le piratage, le terrorisme, les pandémies, etc. L'identification de ces incidents permet d'évaluer leurs impacts sur les activités du CSSD et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

9. FORMATION, SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur l'adoption de comportements sécuritaires et la responsabilisation individuelle.

À cet égard, les membres du CSSD doivent être sensibilisés :

- À la sécurité de l'information et des systèmes d'information du CSSD;
- Aux conséquences d'une atteinte à la sécurité des actifs informationnels;
- À leur rôle et à leurs responsabilités en la matière.

Le CSSD 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 la sécurité de ces actifs ainsi qu'à leur rôle et leurs obligations en la matière.

L'utilisateur a la responsabilité de participer à ces activités de sensibilisation et de formation.

10. RÉVISON DE LA POLITIQUE

La politique sera révisée au minimum tous les 3 ans à compter de sa date d'adoption.

11. ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur à la date de son adoption par le conseil d'administration.