SAINTE-ANNE

PRIMAIRE | SECONDAIRE | COLLÉGIAL

Politique de sécurité des technologies de l'information

Version	Date	Par	Type	Changements
1.0		Amar Lakhdari Kamel Chraiti	Création	Création et adoption par le conseil d'administration

Table des matières

1. Préambule

Le monde d'aujourd'hui n'a plus de frontières et l'espace numérique est à la merci d'actions frauduleuses : vol d'informations personnelles, cyberintimidation, perte de donnée. Notre Collège et ses systèmes d'information sont donc une cible potentielle.

Cette Politique contribue à l'accomplissement de la mission du Collège, 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 multiple et diversifiée est constituée des renseignements personnels d'élèves, d'étudiants et de membres du personnel, de l'information professionnelle sujette à des droits de propriétés intellectuelles (enseignants et chercheurs) et, finalement, de l'information stratégique ou opérationnelle pour l'administration du Collège. Nous sommes interconnectés avec le monde, dans un environnement technologique en changement constant. Une gestion de la sécurité de l'information qui s'adapte à ces transformations est indispensable.

C'est dans ce contexte que le Cégep met en place la présente Politique qui oriente et détermine l'utilisation appropriée et sécuritaire des technologies de l'information.

2. Cadre légal et administratif

Le cadre légal et administratif de la présente Politique est constitué principalement par les lois canadiennes et québécoises en vigueur.

À cet effet, tout utilisateur, tel que défini dans la section 3, qui est appelé à utiliser, à gérer ou à traiter les actifs informationnels du collège Sainte-Anne doit respecter la normativité qui comprend :

- La Charte des droits et libertés de la personne (LRQ, chapitre C-12).
- Le Code civil du Québec (LQ, 1991, chapitre 64).
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1).
- La Loi sur les archives (LRQ, chapitre A-21.1).
- Le Code criminel (LRC, 1985, chapitre C-46).
- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42).
- La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (LQ 2021, C-25).

3. Définitions

Les termes utilisés dans la présente Politique sont définis ci-après.

Actif informationnel	Ensemble des ressources informationnelles ayant une valeur pour la personne physique ou morale qui en est détentrice, et dont la protection nécessite la mise en place de mesures de sécurité particulières, notamment, information numérique, document numérique, système d'information, documentation, équipement informatique, technologie de l'information, acquis ou constitué par le Collège pour mener à bien sa mission.
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.
Collège	Corporation du collège Sainte-Anne, incluant toutes les écoles : Secondaire Lachine, Secondaire Dorval, Préscolaire primaire Dorval, Préscolaire primaire Outremont et Collégial international Lachine.
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 Collège.
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.
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, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communication, de réception et de traitement de l'information, et tout équipement de télécommunications.
Intégrité	Propriété des données qui ne subissent aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

Irrévocabilité	Caractère définitif d'une information. Une information irrévocable ne peut pas être effacée et son annulation ou sa modification est documentée.
Imputabilité	Principe selon lequel une violation ou une tentative de violation d'un système informatique est attribuée à l'entité qui en est responsable
Logiciel	Ensemble des programmes destinés à effectuer un traitement particulier sur un ordinateur. Le terme logiciel est utilisé pour représenter tous les types de programmes.
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 un sinistre majeur.
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.
Renseignement personnel	Toute information relative à une personne Physique et permet, directement ou indirectement, de l'identifier. Cela peut inclure des informations telles que le nom, l'adresse, le numéro de téléphone, l'adresse électronique, les informations financières, les antécédents médicaux, Scolaires ou professionnels, numéros permettant d'identifier un individu (ex:NAS, Assurance-maladie, Permis de conduire)…
Incident	Événement qui porte atteinte, ou qui est susceptible de porter atteinte, à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.
Utilisateur	Toute personne physique ou morale utilisant ou ayant accès aux actifs informationnels du Collège. Sont considérés comme des utilisateurs les membres du personnel enseignant, les membres du personnel professionnel, les membres du personnel de soutien, les membres du personnel d'encadrement, les élèves, les étudiants et les tiers autorisés (par exemple, des consultants, des fournisseurs, des partenaires).

4. Principes directeurs

4.1. Imputabilité

Le Collège met à la disposition des utilisateurs des équipements informatiques et logiciels dans le cadre de l'exercice de leurs fonctions reconnues par le Collège. Ces derniers assument des responsabilités spécifiques quant à l'utilisation de ces outils et sont redevables de leurs actions. Le Collège prend les mesures nécessaires pour s'assurer de leur usage adéquat.

4.2. Mesures de sécurité

Le Collège met en place des mesures de protection, de détection, de prévention et de correction pour assurer la disponibilité, la confidentialité, l'intégrité et l'irrévocabilité de l'actif informationnel de même que la continuité des activités. Ces mesures préviennent notamment les accidents, l'erreur, la malveillance, l'indiscrétion ou la destruction d'information sans autorisation.

4.2.1 Protection des renseignements personnels

Le droit d'accès aux renseignements personnels des utilisateurs est un pouvoir qui est délégué par la Direction générale et contrôlé par la Direction du développement technologique. Chaque système prévoit des droits d'accès différents selon les catégories de personnel. Les renseignements personnels ne sont utilisés et ne servent qu'aux fins pour lesquels ils ont été recueillis. Des règles de gouvernance en matière de protection des renseignements personnels sont prévues dans une autre politique.

4.2.2 Sensibilisation

Le Collège a mis en place un programme formel et continu de sensibilisation sur la sécurité de l'information à l'intention de tous les utilisateurs. Ils sont régulièrement invités à suivre ces formations. Des campagnes de simulation d'hameçonnage sont effectuées tout au long de l'année afin de tester les réflexes et la vigilance du personnel du Collège. Les formations en cybersécurité font également partie du programme d'intégration des nouveaux employés.

4.2.3 Gestion des accès

Les accès directs aux données et aux systèmes sont attribués aux membres du personnel en fonctionde leurs rôles.

L'accès de l'utilisateur aux ressources doit respecter le principe du moindre privilège. Les droits d'accès doivent être revus périodiquement pour s'assurer qu'ils sont toujours appropriés et alignés sur les besoins des utilisateurs.

Les comptes utilisateurs doivent toujours être associés à un utilisateur unique. Les comptes génériques (compte utilisé par plus d'une personne) ne sont pas autorisés.

4.2.4 Continuité des opérations

Pour assurer une continuité des services des technologies de l'information en cas de sinistre majeur (incendie, cyberattaque, panne de courant prolongée, inondation, malveillance, etc.), la Direction du développement technologique doit élaborer un plan de relève informatique qui permet la reprise des activités du Collège dans un délai raisonnable.

5. Objectifs

La présente Politique a pour objectif d'affirmer l'engagement du Collège à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support numérique ou ses moyens de communication.

Cette politique vise à 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 des télécommunications, pour que toutes les activités pédagogiques et administratives du Collège se déroulent dans les meilleures conditions possibles.

Plus spécifiquement, voici les objectifs en matière de sécurité de l'information :

- Identifier, réduire et contrôler les risques pouvant porter atteinte aux systèmes d'information du Collège en favorisant la participation des utilisateurs dans cette démarche de prévention et en réduisant au strict nécessaire l'accès aux données et aux systèmes.
- Assurer la disponibilité, l'intégrité et la confidentialité de l'information durant tout son cycle de vie ;
- Orienter et déterminer la vision du Collège en matière de la sécurité de l'information.

6. Champs d'application

6.1. Actifs visés

Cette politique s'applique aux actifs informationnels qui appartiennent :

- Au Collège Sainte-Anne et qui sont exploités par celui-ci.
- Au Collège et qui sont exploités par un fournisseur de services ou par un tiers.
- À un fournisseur de services ou à un tiers et qui sont exploités par lui au bénéfice du Collège Sainte-Anne.

Elle s'applique à tous les systèmes informatiques (sur site ou hébergé à l'externe, incluant l'infonuagique) qui traitent les données, y compris tout le matériel informatique ou tout objet connecté qui interagit avec les services informatiques du Collège.

6.2. Personnes visées

La présente Politique s'adresse aux utilisateurs, tels que définis à l'article 3.

6.3. Informations visées

L'information visée est celle que le Collège détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers. Tous les supports sont concernés.

7. Rôles et responsabilités

La présente Politique et son application relèvent de différents intervenants à qui des responsabilités spécifiques sont attribuées.

7.1. Conseil d'administration

Adopte la politique ainsi que ses mises à jour.

7.2. Direction générale

Valide la Politique ainsi que ses mises à jour et recommande son adoption au conseil d'administration.

7.3. Direction du développement technologique

- Définit les orientations institutionnelles en matière de sécurité et d'utilisation des technologies de l'information.
- Développe et met en place des directives, procédures et normes touchant l'utilisation et la sécurité des technologies de l'information.
- Accompagne les gestionnaires du Collège dans la mise en application de la présente Politique.
- Assure la sécurité des technologies de l'information en déployant les mesures nécessaires et appropriées.

- S'assure, au moyen d'ententes contractuelles, que cette politique soit respectée par toute personne physique ou morale qui ne fait pas partie des membres du personnel ou des élèves et étudiants du Collège, mais qui a accès aux actifs informationnels.
- Élabore et met en œuvre le programme de sensibilisation à la sécurité de l'information pour les membres du personnel du Collège.
- Élabore et s'assure du respect d'un code d'éthique pour tous les membres du personnel de la direction du développement technologique.
- Assure la sécurité des services infonuagiques acquis par le Collège, selon le modèle de responsabilité partagée entendu avec le fournisseur. Il s'agit minimalement de la sécurité des informations et des données, des comptes et des identités, des appareils mobiles et des ordinateurs.

7.4. Responsable de la protection des renseignements personnels

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels stipule que la personne qui a la plus haute autorité au sein de l'établissement soit responsable de la protection des renseignements personnels. La responsabilité peut être déléguée par écrit, en tout ou en partie, à un membre du conseil d'administration ou à un membre du personnel de direction. Le responsable de la protection des renseignements personnels a pour fonction de :

- Veiller à assurer le respect et la mise en œuvre de la Loi ;
- Tenir les registres de communications de renseignements personnels sans le consentement de la personne concernée, incluant en cas d'incident de confidentialité ;
- Être consulté lors de l'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité ;
- Être avisé en cas d'incident de confidentialité survenu chez un mandataire ou l'exécutant d'un contrat de service ou d'entreprise ;
- Répondre aux demandes d'accès ou de rectification de renseignements personnels

7.5. Comité sur l'accès à l'information et la protection des renseignements personnels

Le comité est sous la responsabilité du président directeur général du collège qui peut désigner une autre personne pour agir à titre du président du comité. Le comité a pour fonction de :

- Soutenir l'établissement dans l'exercice de ses responsabilités et dans l'exécution de ses obligations à l'égard de la protection des renseignements personnels ;
- Approuver les règles de gouvernance à l'égard des renseignements personnels ;
- Être consulté lors des évaluations de facteurs relatifs à la vie privée pour tout projet d'acquisition, de développement et de refonte d'un système d'information ou d'une prestation électronique de services impliquant des renseignements personnels

7.6. Direction des ressources humaines

- Vérifie, au besoin, les antécédents des candidates et des candidats à l'embauche et des membres du personnel impliqués dans la sécurité de l'information.
- Intervient auprès des membres du personnel concernés en cas d'atteinte à la sécurité des technologies de l'information, en collaboration avec la Direction du développement technologique et les autres intervenantes et intervenants.
- Informe la Direction du développement technologique d'une embauche, d'un changement de fonction et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs

informationnels du Collège.

- Informe tout nouveau membre du personnel de ses obligations découlant de la présente Politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information.

7.7. Direction des ressources matérielles

- Contrôle les accès physiques aux locaux du Collège.
- Gère les moyens d'accès physique (clefs, cartes magnétiques, etc.) aux locaux à accès restreint (salles informatiques, entreposage, etc.) en collaboration avec la direction du développement technologique.

7.8. Personnel d'encadrement

- S'assure que les membres du personnel sous sa responsabilité sont au fait de leurs obligations découlant de la présente Politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information.
- Communique à la direction du développement technologique tout problème d'importance en matière de sécurité de l'information.

7.9. Utilisateur

- Prend connaissance de la Politique et y adhère en respectant les normes, directives et procédures en vigueur en matière de sécurité de l'information.
- Utilise les technologies de l'information mises à sa disposition, aux fins auxquelles elles sont destinées et dans le cadre des accès qui lui sont accordés.
- Informe sa ou son responsable, ou la Direction du développement technologique de toute violation des mesures de sécurité de l'information dont elle ou il pourrait être témoin.

8. Manquement aux règles de la Politique

Le Collège exige de toute personne physique ou morale qui utilise ses actifs informationnels de se conformer aux dispositions de la présente Politique ainsi qu'aux normes, directives et procédures qui s'y rattachent. Le non-respect de cette obligation est soumis au processus de sanctions et aux mécanismes de recours prévus aux règlements et politiques du Collège.

9. Entrée en vigueur

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

10. Révision et diffusion

La Direction du développement technologique procède à l'examen de la Politique et à sa révision en fonction de l'évolution des obligations législatives et réglementaires et l'évolution des pratiques en matière de sécurité de l'information. Elle est responsable de la diffusion de cette politique après son adoption.