Collège de Maisonneuve

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Adoptée le : 17 juin 2019
Lors de la : 328^{o} réunion du conseil d'administration

Table des matières

PRÉAMBULE

La Politique de sécurité de l'information établit les balises nécessaires à la protection de l'information créée, reçue et détenue par le Collège de Maisonneuve dans le cadre de ses activités. Il s'agit, notamment, des renseignements personnels d'étudiants, de membres du personnel et de tierces parties, de l'information professionnelle sujette à des droits de propriété intellectuelle et d'informations stratégiques ou opérationnelles utilisées pour l'administration du Collège.

Par la présente politique, le Collège se conforme à la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* et à la Directive sur la sécurité de l'information gouvernementale faisant état des obligations auxquelles doivent se conformer tous les organismes publics quant à l'adoption, à la mise en œuvre et au suivi de l'application d'une politique de sécurité de l'information.

1. DÉFINITIONS

Actif informationnel – La *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., chapitre C-1.1) définit l'actif informationnel sans égard au support comme étant : « Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, 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 transcrit sous l'une de ses formes ou en un autre système de symboles. » Cette même loi assimile 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.

Confidentialité – Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information – L'ensemble des étapes que franchit une information et qui vont de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou à sa destruction, en conformité avec le calendrier de conservation[1].

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

Intégrité – Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

2. OBJECTIFS

La présente politique a pour objectif de définir les balises permettant au Collège de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient les supports ou les moyens de communication utilisés.

Plus précisément, le Collège doit veiller :

- 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 ;
- à assurer 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 utilisé offre la stabilité et la pérennité voulues ;

[1] Pour les références au plan de classification et au calendrier de conservation, voir la Politique de gestion documentaire.

- à assurer la confidentialité de l'information en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées et aux fins prévues.

3. CADRE LÉGAL ET ADMINISTRATIF

La présente politique s'inscrit principalement dans un contexte régi par les lois et documents suivants :

- *Charte des droits et libertés de la personne* (LRQ, chapitre C-12) ;
- *Code civil du Québec* (LQ, 1991, chapitre 64) ;
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics ;
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03) ;
- *Loi concernant le cadre juridique des technologies et l'information* (LRQ, chapitre C-1.1) ;
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1) ;
- *Loi sur les archives* (LRQ, chapitre A-21.1) ;
- *Loi sur l'administration publique* (LRQ, chapitre A-6.01) ;
- *Loi sur la fonction publique* (LRQ, chapitre F-3.1.1) ;
- *Loi canadienne sur les droits de la personne* (LRC. (1985), chapitre H-6) ;
- *Code criminel* (LRC. (1985), chapitre C-46) ;
- *Loi sur le droit d'auteur* (LRC. (1985), chapitre C-42) ;
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2) ;
- Directive sur la sécurité de l'information gouvernementale.

4. CHAMPS D'APPLICATION

La présente politique s'adresse aux utilisateurs, c'est-à-dire à tous les membres du personnel, peu importe leur statut, et à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du Collège ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que le Collège détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

5. ÉNONCÉS DE PRINCIPES GÉNÉRAUX

Protection de l'information

Le Collège adhère aux orientations et aux 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.

Le Collège 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 gestion des risques, 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.

La sécurité des actifs informationnels s'inscrit dans une préoccupation éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

Engagement des utilisateurs

La protection de l'information détenue par le Collège s'appuie sur l'engagement continu de l'ensemble des utilisateurs. Chacun a l'obligation de protéger l'information et le matériel mis à sa disposition. Les utilisateurs ont des responsabilités explicites en matière de sécurité et sont redevables de leurs actions.

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, 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.

Sensibilisation et formation

Le Collège 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 à leurs obligations en la matière.

Droit de regard

Le Collège exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels et des moyens qui permettent d'y accéder.

6. AXES DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents acteurs du Collège par la mise en place d'un cadre de gestion complémentaire à la présente politique permettant notamment une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être remises en question de manière périodique afin 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 Collège s'articule autour de trois axes fondamentaux de gestion. Ces axes sont la gestion des accès, la gestion des risques et la gestion des incidents.

6.1. Gestion des accès

La gestion des accès doit être encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le dessein de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités à tous les membres du personnel et sur l'obligation pour chacun d'eux d'en rendre compte selon leur fonction au sein du Collège.

6.2. Gestion des risques

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse de risques guide également l'acquisition, la conception et l'exploitation des systèmes d'information en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du Collège. La gestion des risques liés à la sécurité de l'information s'inscrit dans le

processus global de gestion des risques du Collège. Les risques à portée gouvernementale sont déclarés, conformément à la Directive sur la sécurité de l'information gouvernementale.

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 auxquels elle est exposée ;
- des conséquences de la matérialisation de ces risques ;
- du niveau de risque acceptable selon le Collège.

6.3. Gestion des incidents

Le Collège 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'atteinte 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.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés conformément à la Directive sur la sécurité de l'information gouvernementale. Dans la gestion des incidents, le Collège peut exercer ses pouvoirs et ses prérogatives en ce qui a trait à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

7. Obligations et responsabilités des intervenants clés en matière de sécurité de l'information

La présente politique détermine les obligations en matière de sécurité de l'information attribuées, notamment, au responsable organisationnel de la sécurité de l'information, aux gestionnaires d'entités administratives et aux utilisateurs.

Le conseil d'administration
Approuve la présente politique ainsi que ses mises à jour.

Le directeur général
Est le premier responsable de la sécurité de l'information relevant de son autorité et assure la mise en œuvre de la présente politique.

Le directeur des ressources informationnelles (responsable de la sécurité de l'information)
Propose au Collège des orientations stratégiques et des priorités d'intervention. Est responsable de l'application, du suivi et de la mise à jour de la présente politique.

Les membres du personnel d'encadrement
S'assurent de la sécurité de l'information et des ressources qui la sous-tendent relevant de la responsabilité de leur unité administrative. Ces gestionnaires sont ainsi responsables de la mise en œuvre des dispositions de la présente politique et des directives qui en découlent auprès du personnel relevant de leur autorité.

Les utilisateurs
Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le Collège.

À cette fin, il doit :

- prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et s'y conformer ;

- dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, utiliser 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 son poste de travail et sur tout appareil contenant des données à protéger et ne pas modifier leur configuration ni 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 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 Collège ;
- au moment de son départ du Collège, remettre les actifs informationnels ainsi que tout le matériel informatique ou de téléphonie mis à sa disposition dans le cadre de l'exercice de ses fonctions.

8. SANCTION

Tout membre de la communauté collégiale qui contrevient à la présente politique s'expose à des sanctions 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 du Règlement sur les sanctions applicables en cas d'infraction à certaines conditions de vie au Collège.

9. DISPOSITIONS FINALES

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration.