COLLÈGE MONTMORENCY

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

DIRECTION DES TECHNOLOGIES DE L'INFORMATION

JUIN 2021

TABLE DES MATIERES

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

1. CONTEXTE

Cette politique constitue un élément essentiel à la gouvernance de l'information permettant ainsi au Collège Montmorency d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qui est traitée, produite et communiquée. Cette information est très vaste et peut exister sur support papier ou technologique. Elle comprend, entre autres, les renseignements personnels des étudiants et des membres du personnel, la propriété intellectuelle produite par les enseignants et les chercheurs, ainsi que la documentation interne stratégique et administrative.

Comme toute autre institution d'enseignement supérieur, le Collège fait face à une multitude de menaces pouvant porter atteinte à la confidentialité, l'intégrité et la disponibilité de son information. Ces menaces, dont la nature est en constante évolution, comprennent, entre autres, le vol d'identité et d'information confidentielle, la fraude, l'espionnage industriel et le vol de propriété intellectuelle, l'utilisation, la divulgation et la destruction d'information, les défaillances techniques, les événements naturels et l'erreur humaine.

Dans ce 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 (LRQ, chapitre. G-1.03) et de la Directive sur la sécurité de l'information crée des obligations aux établissements collégiaux en leur qualité d'organismes publics. Ainsi, la Directive sur la sécurité de l'information gouvernementale oblige le Collège à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de sécurité de l'information 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.

2. DÉFINITION

Actifs informationnels

Tout système ou équipement permettant le traitement, le transport et l'entreposage de toute forme de communication ou d'information. Notamment, les équipements informatiques (poste de travail, ordinateur portatif, imprimante, etc.), les réseaux de communication (Internet, réseau local, réseau sans fil, réseau étendu, etc.), les systèmes de téléphonie et de télécommunication, le courrier électronique, les bases de données, les applications informatiques et les progiciels ainsi que la documentation nécessaire à leur bon fonctionnement. Inclus aussi toutes les informations inscrites sur support papier, électronique ou autres produites ou reçues dans le cadre des opérations.

Utilisateurs

Tout le personnel, toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant, d'administrateur ou de public, utilise les actifs informationnels du Collège.

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.

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.

3. OBJECTIF

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 les supports ou les moyens de communication utilisés.

Plus précisément, le Collège doit veiller à assurer :

- La disponibilité de l'information pour qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- L'intégrité de l'information afin 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;
- La confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées et aux fins prévues, surtout si elle constitue des renseignements personnels.

Par conséquent, le Collège 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 de l'institution.

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 Collège en matière de réduction du risque associé à la protection de l'information.

4. CADRE LÉGAL ET ADMINISTRATIF

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);
- 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, chapitre G-1.03);
- 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);
- La Loi sur les archives (LRQ, chapitre A-21.1);
- 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).

5. CHAMP D'APPLICATION

La présente politique s'applique aux utilisateurs de l'information, 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, de fournisseur ou d'étudiant, utilise les actifs informationnels du Collège.

Tous les supports, qu'ils soient numériques ou papiers, sont concernés.

Les actifs informationnels visés sont ceux que le Collège détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

Les activités visées par la Politique sur la sécurité de l'information sont la collecte, la consultation, la production, la transmission, la conservation et la destruction de l'information et des actifs informationnels, peu importe leur support, leur emplacement et le moyen de communication.

6. PRINCIPES DIRECTEURS

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

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.

Imputabilité

Chaque direction ou service administratif est imputable de la gestion des risques à la sécurité de l'information en sa qualité de propriétaire de l'information. Cette imputabilité s'applique aux actifs informationnels, aux processus et aux systèmes sous sa responsabilité ou son contrôle, incluant ceux délégués à un tiers.

Risque acceptable

Des mesures sont mises en place pour garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels, à un coût proportionnel à la sensibilité de l'information et aux risques sous-jacents ainsi que différents types d'information pouvant nécessiter des niveaux de protection différents. La mise en place du cadre de gestion étant un moyen d'ajuster le risque, par une combinaison de mesures raisonnables mises en place pour garantir la sécurité de l'information, à un coût proportionnel à la sensibilité de l'information et aux effets potentiels. D'autre part, les mesures mises en place pour protéger les actifs informationnels ne doivent pas nuire à la mission du Collège.

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.

Sensibilisation et formation

Former et sensibiliser les utilisateurs à des principes éthiques visant à assurer le code de conduite et la responsabilisation individuelle, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et à leurs obligations en la matière. Chaque individu qui a accès à l'information est responsable de respecter les critères de disponibilité, d'intégrité et de confidentialité de celle-ci.

Cette politique s'inscrit avant tout dans l'esprit qu'une personne avisée en vaut deux et que la sécurité de l'information est l'affaire de tous. Ainsi, l'éducation des usagers, par diverses méthodes d'apprentissage pertinentes à la sécurité de l'information, est un élément significatif de l'ensemble des mesures contribuant à sécuriser davantage l'information du Collège Montmorency.

7. CADRE DE GESTION

La politique confère la reconnaissance et la légitimité à la direction du Collège de définir des directives, des procédures, des guides en lien avec la sécurité de l'information. L'ensemble de ces documents fait partie du cadre de gestion qui a pour objectif d'aligner les opérations dans l'esprit de la présente politique. Puisque le domaine de la sécurité informationnelle est en constante évolution, le cadre de gestion permettra au Collège de s'adapter aux nouvelles réalités de façon efficace et continue et ce, dans la poursuite de sa mission tout en répondant à ses obligations.

8. RÔLES ET RESPONSABILITÉS

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités de chacun des intervenants du Collège par la mise en place d'un cadre de gestion de la sécurité permettant notamment une reddition de comptes adéquate.

La présente politique attribue la gestion de la sécurité de l'information du Collège à des instances, à des comités et à des personnes en raison des fonctions particulières qu'ils exercent.

Conseil d'administration

Le Conseil d'administration adopte la Politique sur la sécurité de l'information ainsi que toute modification à celle-ci. Le Conseil d'administration est régulièrement informé des actions du Collège en matière de sécurité de l'information. Il est le dirigeant de l'organisme responsable de l'application de la Politique sur la sécurité de l'information et il en délègue la responsabilité au directeur général.

Comité de direction

Le Comité de direction du Collège détermine des mesures visant à favoriser l'application de la politique et des obligations légales du Collège en matière de sécurité de l'information. Ainsi, il détermine les orientations stratégiques, les plans d'action et les bilans de sécurité de l'information. Il peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

Direction générale

La Direction générale :

- Veille à l'application de la Politique sur la sécurité de l'information;
- Encadre le responsable de la sécurité de l'information dans la réalisation de son mandat;
- Délègue certaines responsabilités au Secrétaire général pour la gestion de l'information;
- Fait adopter par le Conseil d'administration les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité et les redditions de comptes en matière de sécurité de l'information;
- Autorise, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatibles avec une activité ou un projet directement relié à la mission du Collège et d'en informer le Conseil d'administration;
- Autorise la création d'un comité d'enquête, si une enquête est requise. Cette autorisation au préalable peut provenir de la Direction générale ou de la Direction des ressources humaines;
- Met à jour le registre des dérogations et le registre des cas de contravention à la présente politique;
- Fait le suivi auprès du Comité de direction et du Conseil d'administration.

Responsable de la sécurité de l'information (RSI)

La fonction du RSI est déléguée à un cadre par le Conseil d'administration. Le RSI relève du directeur général au sens du Cadre gouvernemental de gestion de la sécurité de l'information. Cette personne met en place le cadre de gestion de la sécurité de l'information et s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins. Il est nommé par le Conseil d'administration et il peut prendre conseil auprès d'experts du milieu et autres personnes versées en la matière.

Le RSI :

- Formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et met à jour la politique;
- Assure la coordination et la cohérence des actions menées au sein du Collège en matière de sécurité de l'information en conseillant les responsables d'actifs informationnels dans les différents services;
- Propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;
- S'assure de la déclaration, par le Collège des risques et des incidents de sécurité de l'information à portée gouvernementale;
- Collabore à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille au déploiement de ceux-ci;
- Procède aux enquêtes dans des transgressions sérieuses ayant trait présumément à la politique à la suite de l'autorisation du dirigeant de l'organisme;
- S'assure des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

Direction des technologies de l'information

En matière de sécurité de l'information, la Direction des technologies de l'information (ci-après la DTI) 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 développement ou d'acquisition de systèmes d'information dans lesquels elle intervient :

- Elle participe activement à l'analyse de risques, 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 d'information faisant appel aux technologies de l'information;
- Elle applique des mesures appropriées à toute menace ou à tout incident de sécurité de l'information;
- Elle participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par le directeur général.

Direction des ressources matérielles

La Direction des ressources matérielles participe, avec le responsable de la sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Collège.

Direction des ressources humaines

En matière de sécurité de l'information, la Direction des ressources humaines obtient de tout nouvel employé du Collège, après lui en avoir montré la nécessité, son engagement au respect de la politique.

Dans des cas particuliers et selon l'ampleur de la situation, une enquête pourrait être requise. La Direction des ressources humaines pourra autoriser la création d'un comité d'enquête et identifier les membres du comité en question. Cette autorisation au préalable peut provenir de la Direction générale ou de la Direction des ressources humaines. Autrement, s'il est jugé qu'une enquête n'est pas requise, le droit de gérance, c'est-à-dire la possibilité de mettre en place les mécanismes adéquats et nécessaires, pourra alors s'appliquer à la situation.

Responsables d'actifs informationnels

Les responsables d'actifs informationnels sont les cadres détenant l'autorité au sein de leur direction ou service et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels qui sont sous leur responsabilité. Les responsables d'actifs informationnels peuvent déléguer la totalité ou bien une partie de leur responsabilité à un autre membre de leur direction ou service.

Les responsables d'actifs informationnels :

- Informent le personnel relevant de leur autorité et les tiers avec lesquels transige le service de la Politique sur la sécurité de l'information et des dispositions du cadre de gestion dans le but de sensibiliser à la nécessité de s'y conformer;
- S'assurent que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;
- Collaborent activement à la catégorisation de l'information de la direction ou service sous sa responsabilité et à l'analyse de risques;
- Voient à la protection de l'information et des systèmes d'information qui sont sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la Politique sur la sécurité de l'information et de tout autre élément du cadre de gestion;
- S'assurent que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voient à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion;
- Rapportent à la DTI toute menace ou tout incident afférant à la sécurité de l'information;
- Collaborent à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'information;
- Rapportent au directeur général tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de cette politique.

Utilisateurs

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs des actifs informationnels du Collège.

Tout 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 protéger cette information.

À cette fin, l'utilisateur doit :

- Se conformer à la présente politique et à toute autre directive du Collège en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- Utiliser les droits d'accès qui lui sont attribués et autorisés, utiliser l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- Participer à la catégorisation de l'information de son service;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- Signaler au responsable des actifs informationnels de son service tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du Collège;
- Collaborer à toute intervention visant à indiquer ou à mitiger une menace à la sécurité de l'information ou un incident de sécurité de l'information.

Aussi, tout utilisateur du Collège doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

9. SANCTIONS

En cas de contravention à la présente politique, l'utilisateur engage sa responsabilité personnelle; il en est de même pour la personne qui, par négligence ou par omission volontaire, fait en sorte que l'information n'est pas protégée adéquatement.

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l'information qui en découlent, 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.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au Collège ou en vertu des dispositions de la législation applicable en la matière.

10. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le RSI, assisté du comité de travail pour la sécurité de l'information, est responsable de la diffusion et de la mise à jour de la politique. La Politique sur la sécurité de l'information sera révisée au plus tard cinq ans après son adoption.

11. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le Conseil d'administration en date du 8 décembre 2021.