POL-15 Politique sur la sécurité de l'information

Adoptée par le Conseil d'administration le 25 septembre 2017.

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION[1]

TABLE DES MATIÈRES

[1] Dans ce document, l'utilisation du masculin pour désigner des personnes a comme seul but d'alléger le texte et identifie sans discrimination les individus des deux sexes.

Article 1 PRÉAMBULE

Cette politique permet au Cégep Garneau d'accomplir sa mission, 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 est multiple et diversifiée : renseignements personnels d'étudiants et de membres du personnel, information professionnelle sujette à des droits de propriété intellectuelle (professeurs et chercheurs), information stratégique ou opérationnelle pour l'administration du Cégep.

L'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale* crée des obligations aux établissements en leur qualité d'organismes publics. Ainsi, la *Directive sur la sécurité de l'information gouvernementale* oblige le Cégep à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique sur la 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.

Article 2 DÉFINITIONS

a) « Actif informationnel »
Une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le Cégep habituellement accessible ou utilisable avec un dispositif des technologies de l'information (logiciels, progiciels, didacticiels, banques de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un media informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

b) « Cadre de gestion»
L'ensemble des consignes qu'elles soient les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues qui encadrent les activités d'un établissement qu'est un cégep.

c) « Confidentialité »
La propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

d) « 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, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

e) « Plan de continuité »
L'ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité du Cégep.

f) « Responsable d'actifs informationnels »
Le membre du personnel cadre détenant la plus haute autorité au sein d'une unité pédagogique ou administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité.

g) « Risque de sécurité de l'information »
Le degré d'exposition d'une information ou d'un système d'information à une menace d'interruption ou de réduction de la qualité des services ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et qui peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ou sur l'image du Cégep.

Article 3 OBJECTIFS

La présente Politique a pour objectif d'affirmer l'engagement du Cégep à s'acquitter de ses obligations à l'égard de la sécurité de l'information, quel que soit son support ou ses moyens de communication. Plus précisément le Cégep doit veiller à:

- la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;

- 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 de cette information lui procure 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, surtout si elle constitue des renseignements personnels.

Par conséquent, le Cégep se dote d'une politique visant à orienter et à déterminer sa vision qui sera détaillée par le cadre de gestion de la sécurité de l'information de l'institution.

Ce cadre 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 Cégep en matière de réduction du risque associé à la protection de l'information.

Article 4 CADRE LÉGAL ET ADMINISTRATIF

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

- la *Charte des droits et libertés de la personne* (RLRQ, c. C-12);
- le *Code civil du Québec*;
- le *Code criminel* ;
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) et ses règlements;
- la *Directive sur la sécurité de l'information gouvernementale*;
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) et ses règlements;
- la *Loi sur les archives* (RLRQ, c. A-21.1);
- la *Loi sur le droit d'auteur* (RLRC, 1985, c. C-42).

Dans le cadre administratif du Cégep :

Le *Règlement sur la protection des renseignements personnels* (R-07);

Le *Règlement concernant la gestion des documents administratifs et des archives* (R-11);

Le *Code de conduite des utilisateurs des actifs informatiques*.

Article 5 CHAMP D'APPLICATION

La présente Politique s'applique aux utilisateurs de l'information : tout le personnel, toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou d'invité utilise les actifs informationnels du Cégep.

L'information visée est celle que le Cégep détient dans le cadre de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

Tous les supports d'information, incluant le papier, sont concernés.

Article 6 PRINCIPES DIRECTEURS

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

1. identifier l'information à protéger, ses caractéristiques de sécurité et désigner les personnes qui en sont responsables;
2. s'appuyer sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires;
3. adhérer à une approche basée sur le risque acceptable;
4. protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle jusqu'à sa destruction éventuelle;
5. mettre en place une gestion de la sécurité de l'information qui répond au changement constant de l'environnement technologique;
6. évaluer régulièrement les risques, mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, définir des actions d'éradication des menaces ou de recouvrement des activités compromises;
7. adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de sécurité de l'information avec le réseau de l'éducation et les organismes publics;
8. adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle;
9. s'assurer que chaque employé ait accès à seule l'information pertinente pour la réalisation de ses tâches normales;
10. s'assurer d'une communication efficace dans les situations pouvant affecter les actifs informationnels et être identifiées comme des menaces;
11. mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels.

Article 7 CADRE DE GESTION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents acteurs du Cégep par la mise en place d'un cadre de gestion de la sécurité 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 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 sur la sécurité de l'information* du Cégep s'articule autour de trois axes fondamentaux de gestion. Ces axes sont :

- la gestion des accès;
- la gestion des risques;
- la gestion des incidents;

7.1 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 et sur l'imputabilité des personnes, à tous les niveaux de personnel du Cégep.

7.2 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, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du Cégep. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Cégep. 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 par le Cégep.

7.3 Gestion des incidents

Le Cégep 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.

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 Cégep peut exercer ses pouvoirs et ses prérogatives eu égard à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

Article 8 RÔLES ET RESPONSABILITÉS

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

8.1 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 nomme le Responsable de la sécurité de l'information (RSI) tel que requis par la Loi. Il est informé des actions du Cégep en matière de sécurité de l'information.

8.2 Directeur général

Le directeur général est responsable de l'application de la *Politique sur la sécurité de l'information*.

- Il 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 incompatible avec une activité ou un projet directement relié à la mission du Cégep;
- Il autorise une enquête lorsqu'il y a ou pourrait y avoir transgression de la Politique.

8.3 Direction générale

La direction générale du Cégep adopte des mesures visant à favoriser l'application de la Politique et des obligations légales du Cégep en matière de sécurité de l'information. Ainsi, elle détermine les orientations stratégiques, les plans d'action et reçoit les bilans de sécurité de l'information.

8.4 Responsable de la sécurité de l'information (RSI)

Le RSI est nommé par le Conseil d'administration. Il relève du directeur général au sens du *Cadre gouvernemental de gestion de la sécurité de l'information.* Cette personne :

- élabore et propose le cadre de gestion de la sécurité de l'information du Cégep et rend compte de son implantation à la Direction générale;
- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les règles et les bonnes pratiques en matière de sécurité de l'information et propose des mises à jour de la Politique;

- assure la coordination et la cohérence des actions menées au sein du Cégep en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans les unités;
- produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information;
- 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 Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- 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 relatives à des transgressions réelles ou présumées ayant trait à la Politique, à la suite de l'autorisation du directeur général;
- tient à jour le registre des dérogations et le registre des cas de contravention à la présente Politique;
- 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.

8.5 Direction des technologies informatiques

En matière de sécurité de l'information, la Direction des technologies informatiques 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 de réaction appropriées à toute menace ou à tout incident de sécurité de l'information;
- elle participe à l'exécution des enquêtes informatiques relatives à des contraventions réelles ou apparentes à la présente Politique, autorisées par le directeur général.

8.6 Direction des finances et des ressources matérielles

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

8.7 Direction des ressources humaines

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

8.8 Responsable d'actifs informationnels

Le responsable d'actifs informationnels est le gestionnaire détenant l'autorité au sein d'un service, 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 peut donc y avoir plusieurs responsables d'actifs informationnels dans un cégep. Le responsable d'actifs informationnels peut déléguer une partie de sa responsabilité à un autre gestionnaire du service.

Le responsable d'actifs informationnels :

- informe le personnel relevant de son 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 le sensibiliser à la nécessité de s'y conformer;
- collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques;
- voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel autorisé en conformité avec la *Politique sur la sécurité de l'information* et de tout autre élément du cadre de gestion;
- s'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de services sous sa responsabilité et voit 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;
- rapporte à la Direction des technologies informatiques toute menace ou tout incident afférant à la sécurité de l'information;
- collabore 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;
- rapporte au RSI 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.

8.9 Utilisateurs

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

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 Cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- 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 de ses fonctions 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;
- signaler au responsable du service ou du département, tout incident susceptible de constituer une contravention à la présente Politique ou de constituer une menace à la sécurité de l'information du Cégep;
- collaborer à toute intervention visant à indiquer ou à atténuer une menace à la sécurité de l'information ou à un incident de sécurité de l'information.

Aussi, tout utilisateur du Cégep doit se conformer aux politiques et aux directives en vigueur au Cégep 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.

Article 9 SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et sur la responsabilisation individuelle. À cet égard, les membres de la communauté du Cégep doivent être sensibilisés :

- à la sécurité de l'information et des systèmes d'information du Cégep;
- aux conséquences d'une atteinte à la sécurité;
- à leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. De plus, des documents explicatifs sont disponibles sur le site Internet du Cégep.

Article 10 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, 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 Cégep ou en vertu des dispositions de la législation applicable en la matière.

Article 11 DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le RSI, assisté par la Direction des communications et des affaires corporatives, est responsable de la diffusion et de la mise à jour de la Politique.

La *Politique sur la sécurité de l'information* est révisée et modifiée au besoin.

Article 12 ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur dès son adoption par le Conseil d'administration et remplace la *Politique de sécurité sur les technologies de l'information et des télécommunications*.