N/Réf. : G6 111 115

Politique sur la sécurité de l'information du Cégep de Chicoutimi

Cégep de Chicoutimi

Octobre 2017

Adoptée : CAD-30.10.2017

Note : L'utilisation des termes génériques masculins dans ce texte ne véhicule aucun préjudice à l'égard des personnes et n'a d'autre but que d'en alléger le contenu.

TABLE DES MATIÈRES

PRÉAMBULE

Dans le cadre sa mission, du maintien de l'intégrité de sa réputation, du respect des lois, de la réduction des risques et de la protection de l'information qu'il a créée ou reçue (dont il est le gardien), le Cégep de Chicoutimi se dote d'une *Politique sur la sécurité de l'information*.

L'information dont il est question est multiple et diversifiée. Elle consiste en des renseignements personnels d'étudiants et de membres du personnel, en de l'information professionnelle sujette à des droits de propriétés intellectuelles (enseignants et chercheurs) et en de l'information stratégique ou opérationnelle pour l'administration du Cégep.

Le monde d'aujourd'hui n'a plus de frontières, il est ouvert à des menaces tangibles même si elles se situent à priori dans un monde virtuel. Notre Cégep, faisant partie du réseau de l'enseignement supérieur, a une image publique à conserver et est donc susceptible d'être une cible potentielle.

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 gouvernementale*** (une directive du Conseil du trésor du Québec applicable aux cégeps) crée des obligations aux établissements collégiaux 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 de sécurité de l'information, dont les principales modalités sont définies dans la directive gouvernementale, 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.

Objectifs

La présente politique a pour objectif d'affirmer l'engagement du Cégep de Chicoutimi à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, peu importe 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 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 Cégep en matière de réduction du risque associé à la protection de l'information.

Cadre légal et administratif

La *Politique sur la sécurité de l'information* 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)*;

Champ d'application

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public, utilise les actifs informationnels du Cégep de Chicoutimi.

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

Tous les supports, **incluant le papier**, sont concernés.

ARTICLE 1 : PRINCIPES DIRECTEURS

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

1.1. s'assurer de bien connaitre l'information à protéger, en identifier les responsables et leurs caractéristiques de sécurité, principe qui confirme l'importance de maintenir à jour l'inventaire des actifs informationnels;

1.2. 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;

1.3. adhérer à une approche basée sur le risque acceptable ainsi la mise en place du cadre de gestion est 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;

1.4. reconnaître l'importance de la Politique sur la sécurité de l'information et du cadre de gestion de la sécurité de l'information qui doit être articulé par une équipe compétente devant définir, mettre en place, opérer et ajuster la gestion de la sécurité de l'information;

1.5. protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;

1.6. reconnaître que l'environnement technologique est en changement constant et interconnecté avec le monde en mettant en place une gestion de la sécurité de l'information qui s'adapte à ces changements;

1.7. reconnaître l'importance d'évaluer régulièrement les risques, de mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, de définir des actions d'éradication des menaces ou de recouvrement des activités compromises;

1.8. protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction**,** le niveau de sécurité pouvant varier au cours du cycle de vie du document;

1.9. adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de la sécurité de l'information avec le réseau de l'éducation et les organismes publics;

1.10. adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle étant entendu que chaque individu qui a accès à l'information est responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci;

1.11. s'assurer que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;

1.12. communiquer de façon transparente au sujet des menaces pouvant affecter les actifs informationnels, afin que chacun puisse comprendre l'importance d'appliquer la sécurité comme on le demande, être informé de telle sorte qu'il puisse reconnaître les incidents de sécurité et agir en conséquence;

1.13. mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels à sa clientèle, selon un temps prévu.

ARTICLE 2 : 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 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 et la gestion des incidents.

ARTICLE 3 : GESTION DES ACCÈS

La gestion des accès doit être encadrée et contrôlée afin que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le but 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 une imputabilité des personnes, de toutes les classes d'emploi du Cégep.

ARTICLE 4 : 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 :

4.1 de la nature de l'information et de son importance;

4.2 des probabilités d'accident, d'erreur ou de malveillance auxquelles elle est exposée;

4.3 des conséquences de la matérialisation de ces risques;

4.4 du niveau de risque acceptable par le Cégep.

ARTICLE 5 : 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 :

5.1. limiter l'occurrence des incidents en matière de sécurité de l'information;

5.2. gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations;

5.3. amasser des statistiques afin de bâtir des plans de prévention et d'éviter ou de minimiser le retour de ces incidents.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale* (par le CERT/AQ).

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 6 : 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.

6.1. **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 est régulièrement informé des actions du Cégep 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*.

Le comité exécutif du conseil d'administration peut prendre des décisions dans un cadre déterminé préalablement par ce dernier.

6.2. **Comité de direction**

Le comité de direction du Cégep détermine des mesures visant à favoriser l'application de la politique et des obligations légales du Cégep 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. À titre indicatif, les directives découlant de la Politique sur la sécurité de l'information sont notamment la directive de gestion des accès, la directive de gestion des appareils mobiles, la directive de l'utilisation de l'infonuagique et la directive de l'utilisation des médias sociaux.

6.3. **Comité-conseil pour la sécurité de l'information**

Le comité-conseil pour la sécurité de l'information a comme objectif d'assister le responsable de la sécurité de l'information (RSI) dans la mise en place du cadre de gestion de la sécurité de l'information et autre élément pouvant être nécessaire pour assurer la protection du Cégep et être conforme à la réglementation.

C'est aussi un forum d'échange sur la mise en place du cadre de gestion, des plans d'action et des bilans de sécurité de l'information, des activités de sensibilisation ou de formation ainsi que toute proposition d'action en matière de sécurité de l'information.

Le comité sera formé de personnes désignées par le Cégep, tout en respectant les mécanismes prévus, et le responsable de la sécurité de l'information (RSI), qui seront directement concernées ou qui participent au projet de mise en place de la sécurité de l'information.

6.4. **Directeur général**

Le directeur général veille à l'application de la *Politique sur la sécurité de l'information*.

Cette personne aura pour tâche :

6.4.1. d'encadrer le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat;

6.4.2. de déléguer certaines responsabilités au secrétaire général pour la gestion de l'information;

6.4.3. de faire adopter par le conseil d'administration les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information;

6.4.4. d'autoriser, 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;

6.4.5. d'autoriser une enquête, via le RSI, lorsqu'il y a ou pourrait y avoir transgression de la politique;

6.4.6. de tenir à jour le registre des dérogations et le registre des cas de contravention à la présente politique.

6.5. **Responsable de la sécurité de l'information (RSI)**

Le conseil d'administration délègue la fonction de RSI au directeur des ressources informationnelles. 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.

Le RSI :

6.5.1. élabore et propose le programme de sécurité de l'information du Cégep, rend compte de son implantation au comité de direction;

6.5.2. 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;

6.5.3. 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;

6.5.4. produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information;

6.5.5. 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;

6.5.6. s'assure de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);

6.5.7. 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;

6.5.8. procède aux enquêtes dans des transgressions sérieuses ayant trait vraisemblablement à la politique à la suite de l'autorisation du dirigeant de l'organisme;

6.5.9. 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.

6.6. **Direction des ressources informationnelles**

En matière de sécurité de l'information, la Direction des ressources informationnelles 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 il intervient :

6.6.1. 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;

6.6.2. il applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, telles que l'interruption ou la révocation temporaire, lorsque les circonstances l'exigent, 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;

6.6.3. il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par le directeur général.

6.7. **Direction des services administratifs**

La Direction des services administratifs 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 Cégep.

6.8. **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. Elle travaille activement à respecter la directive sur le changement de statut des employés (gestion des accès).

6.9. **Responsable d'actifs informationnels (coordonnateur cadre)**

Le responsable d'actifs informationnels est le cadre 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 la totalité ou bien une partie de sa responsabilité à un autre membre du service, mais doit en informer l'ensemble des intervenants participant à l'application de la politique. Cette responsabilité se doit être attribuée à une personne avec l'expérience nécessaire dans son domaine de travail ou de son service.

Le responsable d'actifs informationnels :

6.9.1. informe le personnel relevant de son autorité et les tiers avec lesquels transige son 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;

6.9.2. collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques;

6.9.3. 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 relevant de son autorité en conformité avec la *Politique sur la sécurité de l'information* et de tout autre élément du cadre de gestion;

6.9.4. 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 service 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;

6.9.5. rapporte au Service des technologies de l'information toute menace ou tout incident afférant à la sécurité de l'information;

6.9.6. 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;

6.9.7. rapporte au responsable de la sécurité de l'information (RSI) tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

6.10. **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 :

6.10.1. 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[1];

6.10.2. utiliser les droits d'accès qui lui sont attribués et autorisés, l'information, les actifs informationnels 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;

6.10.3. utiliser les équipements RI avec soin afin d'en assurer leur durée de vie utile prévue;

6.10.4. collaborer à la catégorisation de l'information de son service;

6.10.5. recourir à la Direction des ressources informationnelles pour modifier, détruire, installer et acheter des programmes, systèmes ou logiciels; pour modifier ou déplacer, détruire, acheter ou installer des composantes matérielles aux ordinateurs et périphériques; pour modifier les configurations des ordinateurs, périphériques et appareils de télécommunication ou mobile du Cégep;

6.10.6. respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;

6.10.7. 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 Cégep;

6.10.8. 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 Cégep 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.

ARTICLE 7 : SENSIBILISATION ET INFORMATION

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

7.1. à la sécurité de l'information et des systèmes d'information du Cégep;

7.2. aux conséquences d'une atteinte à la sécurité;

7.3. à leur rôle et à leurs responsabilités en la matière.

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

ARTICLE 8 : SANCTIONS

En cas de contravention à la présente politique, l'utilisateur engage sa responsabilité professionnelle; 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, des règles disciplinaires internes applicables ou des conventions collectives.

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.

8.1. **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 besoin après son adoption.

ARTICLE 9 : ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration, soit le 30 octobre 2017.

[1]Actif informationnel

Équipements informatiques, audiovisuels et/ou de télécommunication, serveurs, ordinateurs, postes de travail, tablettes numériques, téléphones intelligents, systèmes d'information, de téléphonie, de reprographie, de télécopie, logiciels, progiciels, banques de données et information (textuelle, sonore, symbolique ou visuelle) placée dans un équipement ou sur un média informatique, système de courrier électronique, les réseaux et leurs infrastructures, les accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception, de traitement de l'information, fichier, document et dossier numérique.