View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by ÉDUQ

Cégep André-Laurendeau

Politique sur la sécurité de l'information

Politique adoptée au Conseil d'administration le 29 novembre 2017.

TABLE DES MATIÈRES

1. PRÉAMBULE 3
2. OBJECTIFS 3
3. FINALITÉS 4
4. CHAMP D'APPLICATION 4
5. DÉFINITIONS 5
6. CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION 6
7. GESTION DES ACCÈS 6
8. GESTION DES RISQUES 6
9. GESTION DES INCIDENTS 7
10. RÔLES ET RESPONSABILITÉS 7
11. SANCTIONS 9
12. DISPOSITIONS GÉNÉRALES 10

Note : 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.

1. PRÉAMBULE

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et de la Directive sur la sécurité de l'information gouvernementale[1] créent 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 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.

Cette politique permet au Cégep André-Laurendeau de s'acquitter de ses obligations légales et réglementaires. Elle permet aussi la mise place de mécanismes servant à réduire les risques liés à la gestion de l'information qu'il a produite ou reçue. Cette information est multiple et diversifiée. Elle consiste notamment 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, finalement, en de l'information stratégique ou opérationnelle pour l'administration du Cégep.

2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Cégep à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus spécifiquement, le Cégep doit veiller à:

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

2.2 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;

2.3 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.

De plus, un Cadre de gestion de la sécurité de l'information[2] structure 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.

[1] LRQ, chapitre G1.03

[2] Directive du Conseil du trésor du Québec sur les risques à portée gouvernementale et applicable aux cégeps. Cette directive a été émise en 2014

3. FINALITÉS

La Politique de la sécurité de l'information demande la mise en place de mécanismes permettant de:

3.1 Reconnaître identifier, réduire et contrôler les risques pouvant porter atteinte aux informations propres au collège;

3.2 Reconnaître, identifier et réduire les risques en regard des informations propres à la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif de la clientèle étudiante, du personnel ou de tout partenaire d'affaires du collège;

3.3 Assurer la gestion des accès (disponibilité et révocabilité);

3.4 Assurer la surveillance et l'intégrité des réseaux informatiques, des télécommunications, d'Internet et des actifs informationnels;

3.5 Assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatif à la clientèle étudiante, au personnel du collège et à tout partenaire d'affaires du collège provenant du milieu des affaires ou de l'industrie ;

3.6 Assurer la conformité aux lois et règlements applicables ;

3.7 Établir un plan de continuité et de relève des services informatiques du collège.

4. CHAMP D'APPLICATION

La présente politique s'adresse à tous les utilisateurs tels que définis à la section suivante.

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.

Le collège, en tant que personne morale, est propriétaire de l'actif informationnel.

5. DÉFINITIONS

5.1 **Actif informationnel** : l'information acquise ou générée par le Cégep pour mener à bien sa mission, peu importe son support, ainsi que les systèmes et équipements utilisés pour son traitement, son utilisation, son stockage, sa conservation et sa communication.

5.2 **Information** : renseignements consignés sur un support quelconque (papier ou électronique) qui est utilisé dans le but de transmission de connaissances. À titre d'exemple, l'information comprend notamment les fichiers structurés tels que les bases de données et ceux non structurés tels que les fichiers des traitements de textes ou ceux des tableurs. On ajoute à cette liste : les courriels, les messages textes, les communications et les messages vocaux, photos, dessins, télécopies, originaux et copies de documents papier, rapports informatisés ainsi que les copies de sauvegarde et les archives. Les dossiers étudiants ou ceux des employés sont aussi considérés comme de l'information.

La perte, le vol ou la destruction de tels actifs pourrait causer préjudice au Cégep. Une information est qualifiée d'actif informationnel lorsqu'elle répond à un ou plusieurs de ces critères :

5.2.1 Il est engendré par les opérations administratives et/ou les activités académiques du Cégep;

5.2.2 Il sert à la planification, la gestion, l'exploitation, le contrôle ou la vérification d'une fonction du Cégep;

5.2.3 Il entre dans la composition de documents officiels du Cégep**.**

Des exemples d'actifs informationnels sont le dossier étudiant et les dossiers des membres du personnel, les différents rapports produits par le Cégep, les plans-cadres, les plans de cours, etc.

5.3 **Utilisateur** : étudiant, membre du personnel ou 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.

5.4 **Risque à la sécurité de l'information**. Tout événement comportant 1° d'incertitude, qui pourrait porter atteinte à la confidentialité, l'intégrité ou à la disponibilité de l'information et causer un préjudice au collège.

5.5 **Dossier étudiant.** Dossier contenant généralement la demande d'admission du SRAM, l'avis d'admission du collège, d'anciens bulletins ou relevés de notes, certains documents d'immigration, certains formulaires reliés au cheminement, le certificat de naissance.

5.6 **Dossier des employés.** Dossier contenant généralement le curriculum vitae, les diplômes requis pour l'emploi, les lettres d'embauche, la fiche d'appréciation du personnel, attestations d'emploi, fiche d'adhésion assurance

collective, entente de confidentialité, formulaire d'accès à l'égalité à l'emploi, lettre disciplinaire, date de naissance et numéro d'assurance sociale.

5.7 **Responsable de l'actif informationnel** : Leur rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service.

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

5.9 **CERT/AQ[3] :** Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise

6. CADRE 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 Cégep par la mise en place d'un *Cadre de gestion de la sécurité de l'information* 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.

Dans les sections qui viennent, nous verrons que cette politique 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.

7. 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 une imputabilité des personnes, à tous les niveaux pour l'ensemble des personnels du Cégep.

8. GESTION DES RISQUES

On appelle un risque, tout événement comportant un certain degré d'incertitude et qui pourrait porter atteinte à la confidentialité, l'intégrité ou à la disponibilité de l'information et ainsi causer un préjudice. La gestion des risques est une approche systémique permettant aux gestionnaires de prendre des décisions éclairées en contexte d'incertitude, en considérant les enjeux importants liés aux risques et à la sécurité de l'information.

Une catégorisation des actifs informationnels à jour soutient l'analyse des 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

[3] Computer Emergency Response Team de l'Administration québécoise

Cégep. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*. En général, 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.

9. 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'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 doivent être communiqués à la direction générale et déclarés par le RSI conformément à la *Directive sur la sécurité de l'information gouvernementale*, et ce, en lien avec 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.

10. 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.

10.1 Conseil d'administration

Le conseil d'administration adopte la Politique de sécurité de l'information ainsi que toute modification à celle-ci. Le conseil d'administration désigne un cadre pour la fonction de RSI**.** Le conseil est informé annuellement des actions du Cégep en matière de sécurité de l'information.

10.2 Comité de direction

Le comité de direction du Cégep détermine des mesures visant à favoriser l'application de cette politique et des obligations légales du Cégep en matière de sécurité de l'information. À partir des bilans de sécurité, il détermine les plans d'action, les directives et les procédures qui viennent préciser ou soutenir l'application de la politique. Au besoin, le comité de direction assiste le responsable de la sécurité de l'information (RSI) afin de mettre en place le *Cadre de gestion de la sécurité de l'information* et tout autre élément pouvant être nécessaires pour assurer la protection de l'actif informationnel du Cégep.

10.3 Directeur général

Le directeur général est responsable de l'application de la politique sur la sécurité de l'information. Il a pour tâche :

- D'encadrer le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat;
- De déléguer certaines responsabilités au secrétaire général pour la gestion de l'information;
- D'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique.

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

Le responsable de la sécurité de l'information est usuellement le coordonnateur du Service des technologies de l'information. Il met notamment 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 relève du directeur général pour la réalisation de ce mandat. Il a pour tâche de:

- Élaborer et proposer un *Cadre de gestion de la sécurité de l'information;*
- Rendre compte de son implantation au comité de direction;
- Formuler 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;
- Assurer 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;
- Produire les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information;
- Proposer 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'assurer de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- À la suite de l'autorisation du directeur général, procéder aux enquêtes dans des cas de transgressions sérieuses;
- S'assurer 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.

10.5 Service des ressources matérielles

Le Service des ressources matérielles participe, avec le responsable de la sécurité de l'information, à l'identification et à l'installation des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep. Ce service 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 de la sécurité de l'information*;

10.6 Service des ressources humaines

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

10.7 Responsable d'actifs informationnels

Le responsable des actifs informationnels est obligatoirement un employé-cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif. Le responsable d'actif informationnel :

- Informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de cette et des autres dispositions réglementaires 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 relevant de son autorité en conformité avec la politique de 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 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;
- Informe le service des technologies de l'information 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;
- Informe le directeur général 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.

10.8 Utilisateurs

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs des actifs informationnels. Ainsi, 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 diligente afin de protéger cette information. À cette fin, l'utilisateur :

- Se conforme à la présente politique et à toute autre directive du Cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- Utilise uniquement 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;
- Participe à la catégorisation de l'information de son service;
- Respecte les mesures de sécurité mises en place, ne pas les contourner, ni modifier leur configuration, ni les désactiver;
- Signale au responsable des actifs informationnels de son unité tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du Cégep;
- Collabore 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 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.

11. 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 (conventions collectives de travail et du Règlement du collège).

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.

12. DISPOSITIONS GÉNÉRALES

12.1 Entrée en vigueur

La politique de sécurité de l'information entre en vigueur au moment de son acceptation, par résolution, par le conseil d'administration.

12.2 Diffusion

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 aux bonnes pratiques. À cet égard, le Cégep met en place les moyens de diffusion suivants :

- Cette politique est diffusée auprès de toute la communauté du Cégep dès son entrée en vigueur;
- Des documents explicatifs sont rendus disponibles sur le site Internet du Cégep;
- Des activités de sensibilisation et de formation sont offertes périodiquement.

12.3 Révision

La politique de sécurité de l'information doit être révisée au maximum après cinq (5) ans à compter de son adoption. La révision est déclenchée par la direction générale en appliquant la procédure suivante :

- Le RSI effectue les travaux de révision;
- Un document révisé est soumis au comité de direction pour examen et, le cas échéant, modifications;
- Le comité de direction recommande au conseil d'administration l'adoption de la politique.