COLLÈGE
D'ENSEIGNEMENT GÉNÉRAL ET PROFESSIONNEL
MARIE-VICTORIN

POLITIQUE NUMÉRO 46
PORTANT SUR LA SÉCURITÉ DE L'INFORMATION

Adoptée le 31 janvier 2018
CA-18-224-1881

TABLE DES MATIÈRES

PRÉAMBULE

Conscient de ses responsabilités et soucieux de sa réputation et de son image, le Cégep Marie-Victorin doit adopter, mettre en œuvre, maintenir à jour et 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 de l'accès à l'information, la gestion des risques et la gestion des incidents. Les principales modalités de cette politique s'inspirent de la Directive sur la sécurité de l'information gouvernementale[1].

ARTICLE 1 – DÉFINITIONS

Actif informationnel

Tous les documents créés ou reçus par le personnel du Cégep Marie-Victorin dans le cadre des fonctions et responsabilités de chacun sans égard à la nature (pédagogique, administrative, financière, légale ou autres) et au support et au format (papier, électronique y incluant le web, audiovisuel ou autre) dans lequel ils sont publiés. Ces documents peuvent contenir des informations nominatives et/ou de nature confidentielle

Classification de l'information

L'attribution de la classification revient aux directeurs et gestionnaires des services (propriétaire), qui eux, détermineront les droits d'accès accordés aux usagers sous leur responsabilité. Une information peut être catégorisée sous trois grandes classes en respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., C.A-2.1) :

- Publique : Cette information peut être distribuée sans restriction à l'intérieur comme à l'extérieur du collège. Elle est généralement informative. Sa divulgation ne risque pas de causer des dommages ou préjudices au collège.

- Privée : Cette information est strictement d'usage interne. Les utilisateurs peuvent s'en servir pour effectuer leur travail. Il pourrait y avoir des impacts indirects sur le collège si les informations de cette classe étaient dévoilées au public.

- Confidentielle : L'information de cette catégorie doit être protégée par des obligations légales ou contractuelles. Elle est généralement stratégique. Elle nécessite le plus haut niveau de sécurité.

Cégep

Le Cégep Marie-Victorin.

[1] Gouvernement du Québec, Conseil du Trésor, *Directive sur la sécurité de l'information*, Décret 7-2014 du 15 janvier 2014

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 sa destruction, en conformité avec le calendrier de conservation du Cégep Marie-Victorin. Le cycle de vie d'un document est séparé en trois stades : actif, semi-actif et inactif. Par extension, on parlera de documents actifs, semi-actifs et inactifs.

- Stade actif : Stade où un document est fréquemment consulté et utilisé à des fins pédagogiques, administratives, financières, légales ou autres.
- Stade semi-actif : Stade où un document est occasionnellement consulté et utilisé à des fins pédagogiques, administratives, financières, légales ou autres.
- Stade inactif : Stade où un document n'a plus d'utilité pédagogique, administrative, financière, légale ou autres. Il peut toutefois être conservé pour sa valeur historique.

Intégrité de l'information

Propriété d'une information ou d'une application logicielle en vertu de laquelle elle doit être complète et exacte, n'ayant subi aucune altération lors de son traitement ou son utilisation, et ce, sans autorisation.

Utilisateur

Tout membre du personnel du Cégep, tout étudiant ainsi que toute personne physique ou morale autorisée à utiliser l'Actif informationnel du Cégep.

ARTICLE 2 – OBJECTIFS

Cette politique vise la réalisation des objectifs suivants :

- gérer de façon responsable l'accès et l'intégrité des informations, de même que la protection de la vie privée des individus dans le milieu professionnel, notamment la confidentialité des informations à caractère nominatif concernant le personnel et les étudiants du Cégep;
- identifier, réduire et contrôler les risques pouvant compromettre la sécurité de l'information;
- inciter les Utilisateurs à adopter les bonnes pratiques relatives à l'utilisation et la sécurité des information;
- assurer le respect des normes et des règles en matière d'utilisation et de sécurité de l'information édictées dans les différentes politiques, règlements et directives existantes et en application au Cégep.

ARTICLE 3 – CHAMPS D'APPLICATION

La présente politique s'adresse aux Utilisateurs et concerne la sécurité de l'information, sous toutes ses formes, électronique, écrite ou autre, et peu importe le support utilisé. 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.

La présente politique ne s'applique pas à La Politique institutionnelle sur l'intégrité et la conduite responsable dans la recherche et les travaux d'érudition, cette dernière découlant des lois fédérales.

ARTICLE 4 - PRINCIPES DIRECTEURS

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

- s'assurer de bien connaitre l'information à protéger, en identifier les responsables et les caractéristiques de sécurité;
- protéger rigoureusement les renseignements personnels, ainsi que toute autre information confidentielle;
- protéger l'information tout au long de son Cycle de vie;
- communiquer de façon transparente au sujet des menaces pouvant affecter l'Actif informationnel, afin que chacun puisse comprendre l'importance d'appliquer les règles appropriées de sécurité, être informé de telle sorte qu'il puisse reconnaître les incidents de sécurité et agir en conséquence.

ARTICLE 5 - CADRE DE GESTION

La politique de sécurité de l'information du Cégep s'articule autour de trois axes fondamentaux de gestion :

<u>Gestion des accès</u>

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.

<u>Gestion des risques</u>

Une classification de l'Actif informationnel à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.
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, tel que recommandé par le comité de travail pour la sécurité de l'information

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.

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 afin de :

- 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 au coordonnateur organisationnel de gestion des incidents du Ministère de l'éducation et de l'Enseignement supérieur (COGI-réseau), 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 6 - RÔLES ET RESPONSABILITÉS

Direction générale

Le directeur général veille à l'application de la *Politique portant sur la sécurité de l'information,* et affecte les ressources nécessaires à l'application de la politique, notamment :

- appuyer le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat;
- autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique ayant une incidence directe ou indirecte sur la sécurité de l'information;
- autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique.

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. Il peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

Comité de travail pour la sécurité de l'information

Le comité de travail pour la sécurité de l'information a comme objectif d'assister le responsable de la sécurité de l'information (RSI) à mettre en place le 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.

Le comité TIC institutionnel devient, en complément de ses responsabilités actuelles, le comité de travail pour la sécurité de l'information.

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, tel que mentionné dans le 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 d'appropriation en cette matière répond aux besoins. Le RSI :

- collabore, avec les services concernés, 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;
- produit les plans d'action, les bilans et les redditions de comptes du cégep en matière de sécurité de l'information;
- collabore avec le Service des technologies de l'information relativement à :
    - la formulation de 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;
    - à l'établissement de 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;
    - la déclaration par le cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (COGI-réseau);
- 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;
- procède aux enquêtes dans des transgressions sérieuses présumées ayant trait à la politique à la suite de l'autorisation de la direction générale;
- tient à jour le registre des dérogations et le registre des cas de contravention à la présente politique.

Service des technologies de l'information

Le service des technologies de l'information :

- 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;
- participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre, de même qu'à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information;
- applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, telles que par exemple 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;
- participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par le directeur général.

Responsable de l'Actif informationnel

Le responsable de l'Actif informationnel est le cadre détenant l'autorité au sein d'un service et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité de l'Actif informationnel sous la responsabilité de ce service.

Le responsable de l'Actif informationnel :

- informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de la politique de sécurité de l'information dans le but de le sensibiliser à la nécessité de s'y conformer;
- collabore activement à la classification 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;
- rapporte au 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.

Utilisateurs

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 de l'Actif informationnel;
- 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;
- participer à la classification de l'information de son service, tel que défini à l'article 5;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- signaler au responsable de la sécurité de l'information 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 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 lorsqu'il y partage de l'Actif informationnel, des dispositifs de technologies de l'information ou des systèmes d'information.

ARTICLE 7 - 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, quelle que soit le format dans lequel elle est produite, n'est pas protégée adéquatement.

Tout Utilisateur qui contrevient à la présente politique, y incluant le cadre légal présenté à l'annexe 1, 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 des conventions collectives en vigueur et du règlement numéro 9 relatif aux conditions de vie au Cégep.

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 8 - DISPOSITIONS FINALES

- Le préambule fait partie de la présente politique.
- La présente politique a été adoptée par le Conseil d'administration le _ janvier 2018.
- La présente politique abroge tout autre document ou texte adopté antérieurement concernant les objets de ladite politique.

ANNEXE I - 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);
- le règlement 09 régissant les conditions de vie au Cégep Marie-Victorin;
- la politique 41 sur l'utilisation des TIC;
- la politique 42 sur la gestion documentaire;
- la politique 43 sur l'utilisation et développement des médias sociaux ;
- la directive sur l'utilisation de l'infonuagique.