POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

COTE 6200

OBJET

La présente politique vise à établir l'engagement du Collège de Rimouski 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.

DESTINATAIRES

Toute personne physique ou morale qui fréquente les lieux et les terrains du Collège notamment, les étudiantes et les étudiants, les membres du personnel du Collège, les fournisseurs, les locataires et les visiteuses et les visiteurs.

DISTRIBUTION

Le Cahier de gestion disponible sur le site Web du Cégep de Rimouski

CONTENU

RESPONSABLES DE L'APPLICATION

La Direction générale
La Direction des ressources financières, matérielles et informationnelles

RÉFÉRENCES

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* [LRQ, chapitre. G-1.03]
- *Directives sur la sécurité de l'information gouvernementale*

ADOPTION

La présente politique a été adoptée par le conseil d'administration du Collège de Rimouski le 28 mai 2019 (CA 19-04.17).

1.0 PRÉAMBULE

Cette politique permet au Collège de Rimouski 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, dont il est le gardien. Cette information est multiple et diversifiée. Elle consiste en des renseignements personnels d'étudiantes et d'étudiants ainsi que de membres du personnel, en de l'information professionnelle sujette à des droits de propriétés intellectuelles et, finalement, en de l'information stratégique ou opérationnelle pour l'administration du Collège. La valeur légale, administrative, économique ou patrimoniale de cette information justifie sa protection durant tout son cycle de vie.

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* 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.

2.0 DÉFINITIONS

Actif informationnel : inventaire présentant, à un moment déterminé, le portrait de l'ensemble des ressources informationnelles d'une organisation, à l'exception des ressources humaines. L'actif informationnel peut inclure une banque d'information électronique, un système d'information, une installation ou encore un ensemble de ces éléments acquis ou constitués par une organisation.

Cadre de gestion : ensemble des règlements, des directives, des procédures et des bonnes pratiques reconnues qui encadrent les activités du Collège. La ou le cadre de gestion vise à renforcer la gouvernance de la sécurité de l'information du Collège, en décrivant les rôles et les responsabilités nécessaires à une gestion intégrée de la sécurité de l'information.

Catégorisation : processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder en termes de disponibilité, d'intégrité et de confidentialité.

CERT/AQ : équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale. CERT en anglais : Computer Emergency Response Team.

Confidentialité : propriété d'une information accessible aux personnes désignées et autorisées qui ne peut être divulguée qu'à celles-ci.

Continuité des affaires : capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

Cycle de vie de l'information : ensemble des étapes que franchit l'information, de sa conception en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation du Collège.

Disponibilité : propriété d'une information accessible en temps voulu et de la manière requise par une personne autorisée.

Gestion des risques en sécurité de l'information : processus d'identification, de contrôle et de réduction des risques de sécurité qui pourraient nuire à l'information.

Incident : 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 actifs informationnels, notamment une interruption des services ou une réduction de leur qualité.

Incident de sécurité de l'information à portée gouvernementale : conséquence observable de la concrétisation d'un risque de sécurité nécessitant une intervention concertée au plan gouvernemental.

Intégrité : propriété d'une information qui ne peut subir aucune altération ni destruction sans autorisation ou de façon erronée, et qui est conservée sur un support et préservée avec des moyens lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Mesure de sécurité de l'information : moyen concret assurant partiellement ou totalement la protection d'information du Collège contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs institutionnels, acte involontaire, acte malveillant tel que l'intrusion dans un système informatique, etc.) et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

Renseignement confidentiel : information dont l'accès est assorti d'une ou de plusieurs restrictions, dont celles prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, que sont les incidences sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, l'administration de la justice et de la sécurité publique, les décisions administratives ou politiques, la vérification et les renseignements personnels.

Renseignement personnel : information concernant une personne physique et qui permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la présente politique.

Responsable d'actifs informationnels : 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 sa responsabilité. Aux fins de l'application de la présente politique, il peut s'agir d'une ou d'un autre membre du personnel cadre de l'unité.

Risque de sécurité de l'information : 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 Collège.

Risque de sécurité de l'information à portée gouvernementale : risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, 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, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

3.0 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);
- la *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, r. 02);
- la *Directive sur la sécurité de l'information gouvernementale*.

4.0 OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Collège de Rimouski 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 précisément, il s'agit d'assurer, tout au long du cycle de vie de l'information, sa disponibilité, son intégrité et sa confidentialité et les moyens mis en oeuvre pour l'assurer doivent être proportionnels à sa valeur et aux risques auxquels elle est exposée.

La politique soutient la mise en œuvre du cadre de gestion en matière de sécurité de l'information et renforce le maintien de systèmes de contrôles internes offrant une assurance raisonnable de conformité à l'égard des lois, des directives et des pratiques gouvernementales en la matière.

5.0 CHAMP D'APPLICATION

La présente politique s'adresse aux utilisatrices et aux utilisateurs, c'est-à-dire à tout le personnel, à toute personne physique ou morale qui, à titre d'employée ou d'employé, de consultante ou de consultant, de partenaire, de fournisseur, d'étudiante ou d'étudiant ou de public, accède à l'information ou utilise les actifs informationnels du Collège.

L'information visée est celle que le Collège 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.

Les activités visées par la politique sont notamment la cueillette, la consultation, la production, la transmission, la conservation et la destruction de l'information et des actifs informationnels, peu importe leur support, leur emplacement, le moyen de communication, que ces activités soient conduites dans ses locaux ou dans un autre lieu.

6.0 PRINCIPES DIRECTEURS

6.1 Protection de l'information

Toute information que le Collège détient, traite ou transmet doit faire l'objet de mesures de sécurité visant à :

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

6.2 Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation et de toute utilisation non autorisée.

Au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, sont notamment considérés confidentiels :

- les renseignements personnels;
- tout renseignement dont la divulgation aurait des incidences sur :
  - les relations intergouvernementales;
  - les négociations entre organismes publics;
  - les partenaires relativement à leurs renseignements industriels;
  - l'administration de la justice et la sécurité publique;
  - les décisions administratives ou politiques.

6.3 Continuité des affaires

Le Collège doit disposer d'un processus de la continuité des activités, comprenant un plan de reprise informatique, qui permet de parer à des cas de sinistre ou d'incident majeur touchant la disponibilité de l'information afin de permettre, dans un délai raisonnable, le rétablissement des processus d'affaires et des systèmes d'information jugés essentiels.

6.4 Évolution

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des menaces et des risques.

Les menaces pouvant affecter les actifs informationnels doivent être communiquées de façon transparente afin que chacun puisse reconnaître les incidents de sécurité et agir en conséquence.

6.5 Universalité

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent s'appuyer sur les normes internationales pertinentes, dans la mesure du possible, afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires.

6.6 Éthique

Le processus de gestion de la sécurité de l'information doit être soutenu par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

7.0 CADRE DE GESTION

7.1 Gestion de la sécurité de l'information

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'elles exercent.

La *Politique de sécurité de l'information* du Collège s'articule autour de trois (3) axes fondamentaux de gestion : la gestion des accès, la gestion des risques et la gestion des incidents.

7.1.1 Gestion des accès

Le Collège doit encadrer et contrôler la gestion des accès pour faire en sorte que la divulgation et l'utilisation de l'information soient strictement réservées aux personnes autorisées afin qu'elles puissent accomplir les tâches qui leur sont confiées. 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 utilisatrices et des utilisateurs, à tous les niveaux de l'organisation.

7.1.2 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 Collège. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Collège. 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 auxquelles elle est exposée;
- des conséquences de la matérialisation de ces risques;
- du niveau de risque acceptable pour le Collège.

7.1.3 Gestion des incidents

Le Collège 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 la situation.

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 Collège 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.

7.2 Rôles et responsabilités

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

7.2.1 Directrice générale ou directeur général

La directrice générale ou le directeur général est responsable de l'application de cette politique et le conseil d'administration lui délègue l'autorité d'entreprendre toute action pour en assurer le respect. Plus spécifiquement, la directrice générale ou le directeur général peut :

- se faire assister de tout membre du personnel en lui accordant des mandats pertinents;
- 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 Collège;
- autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique.

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

Le conseil d'administration délègue à une ou un cadre la fonction de RSI et nomme cette dernière ou ce dernier. La ou le RSI est la principale interlocutrice ou le principal interlocuteur en ce qui concerne la sécurité de l'information au Collège et relève de la directrice générale ou du directeur général au sens du *Cadre gouvernemental de gestion de la sécurité de l'information*. Elle ou il veille à l'application de la politique et met en place le cadre de gestion de la sécurité de l'information en s'assurant que le niveau de maturité de ce dernier répond aux besoins. Plus spécifiquement, la ou le RSI :

- collabore étroitement avec le comité de travail sur la sécurité de l'information;
- élabore et propose le programme de sécurité de l'information du Collège et rend compte de son implantation;
- 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 unités;

- produit les redditions de comptes du Collège en matière de sécurité de l'information;
- s'assure de la déclaration par le Collège des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- élabore le 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 à la politique sur autorisation de la directrice générale ou du directeur général;
- suit l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information;
- coordonne la cellule de crise sous l'aspect non technique.

7.2.3 Coordonnatrice ou coordonnateur sectoriel de la gestion des incidents (CSGI)

La ou le CSGI représente le Collège en matière de déclaration des incidents à portée gouvernementale. La ou le RSI désigne la ou les personnes agissant à titre de CSGI. Cette dernière ou ce dernier effectue des tâches concernant la prévention, la réaction et l'amélioration de la sécurité de l'information. Plus spécifiquement, la ou le CSGI :

- analyse les menaces et failles de sécurité et communique l'information aux administratrices et aux administrateurs de systèmes;
- aide à prévenir les incidents de sécurité en proposant des solutions conformes aux bonnes pratiques reconnues;
- aide à identifier les problèmes de sécurité de son organisation;
- propose des échéances d'implantation de correctifs selon la criticité des failles de sécurité décelées;
- participe à la mise en place d'une équipe de réponse aux incidents de sécurité (ERI);
- avec les autres membres de l'ERI, développe, met en place et teste un plan de réponse aux incidents de sécurité;
- coordonne ou participe à la coordination de l'ERI lorsque des incidents de sécurité se produisent;
- communique et échange des informations avec la coordonnatrice ou le coordonnateur organisationnel de gestion des incidents (COGI) de son réseau lors d'incidents de sécurité touchant son organisation.

7.2.4 Comité de travail sur la sécurité de l'information

Le comité a comme objectif d'assister la ou le 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 Collège et être conforme à la réglementation. C'est un comité tactique et opérationnel.

Il est formé des parties prenantes du Collège qui participent au projet de mise en place de la sécurité de l'information. Celles et ceux qui doivent obligatoirement y participer sont les deux (2) CSGI, la ou le RSI, une représentante ou un représentant de l'IMQ, du CFMU et du CMÉC. Ce comité de travail doit tenir au moins deux (2) rencontres annuellement.

7.2.5 Direction des ressources financières, matérielles et informationnelles (DRFMI)

a) Coordination des Technologies de l'information

La coordination des Technologies de l'information s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation ou l'acquisition des systèmes d'information de

même que dans la réalisation de projets de développement dans lesquels elle intervient. Plus spécifiquement, 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;
- applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information;
- participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la directrice générale ou le directeur général.

b) Coordination des Terrains, bâtiments et approvisionnement

La coordination des Terrains, bâtiments et approvisionnement du Collège participe, avec la ou le RSI, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Collège.

7.2.6 Direction des ressources humaines

En matière de sécurité de l'information, la Direction des ressources humaines obtient de toute nouvelle employée ou de tout nouvel employé du Collège, après lui en avoir montré la nécessité, son engagement au respect de la présente politique. De plus, la Direction des ressources humaines doit informer les Technologies de l'information et les Terrains, bâtiments et approvisionnement lors :

- d'une embauche;
- d'un changement de fonction;
- d'une absence : invalidité, congé de maternité ou paternité, congé sans solde, congé différé ou de perfectionnement;
- et de la fin d'emploi d'une personne;

afin de mettre à jour les accès aux actifs informationnels, de permettre la remise des clés et de tout matériel appartenant au Collège.

7.2.7 Responsable d'actifs informationnels

La ou le responsable d'actifs informationnels est la ou 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. Plus spécifiquement, la ou le responsable d'actifs informationnels :

- informe son personnel et les tiers avec lesquels elle ou il transige de la *Politique de sécurité de l'information* et des dispositions du cadre de gestion dans le but de les 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 toute consultante ou tout consultant, fournisseur, partenaire, invitée ou invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion;
- rapporte à la coordination des Technologies de l'information toute menace ou tout incident afférent 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;
- rapporte à la ou au RSI tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'une ou d'un membre du personnel.

7.2.8 Utilisatrices ou utilisateurs

Toute utilisatrice ou tout utilisateur qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'elle ou il en fait et doit procéder de manière à protéger cette information.

À cette fin, l'utilisatrice ou l'utilisateur doit :

- se conformer à la présente politique et à tout autre élément du cadre de gestion en sécurité de l'information;
- utiliser les droits d'accès qui lui sont attribués et autorisés;
- utiliser l'information et les actifs informationnels qui sont mis à sa disposition uniquement aux fins auxquelles ils sont destinés, dans le cadre de ses fonctions;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- signaler à la ou au responsable des actifs informationnels tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du Collège.

8.0 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 Collège doivent être sensibilisés :

- à la sécurité de l'information et des systèmes d'information du Collège;
- 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 doivent être disponibles.

9.0 SANCTIONS

En cas de contravention à la présente politique, l'utilisatrice ou l'utilisateur engage sa responsabilité personnelle; elle ou 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, dont celles des conventions collectives de travail et des règlements du Collège.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, une ou un partenaire, une invitée ou un invité, une consultante ou 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.

10.0 DIFFUSION ET MISE À JOUR DE LA POLITIQUE

La ou le RSI, assisté du comité de travail sur la sécurité de l'information, est responsable de la diffusion et de la mise à jour de la politique. La *Politique de sécurité de l'information* sera révisée au plus tard trois (3) ans après son adoption.

11.0 ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration.