Cégep Limoilou

C-15 Politique sur la sécurité de l'information

Recueil sur la gouvernance

Adopté par le Conseil d'administration le 23 avril 2019 (résolution C.A. 432.05.02)

PRÉAMBULE

Le Cégep Limoilou possède une information multiple et diversifiée qu'il a l'obligation de protéger.

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 (Décret 7-2014) obligent le Cégep à adopter une politique de sécurité de l'information, à la mettre en œuvre, à la maintenir à jour et à en assurer l'application. En plus d'établir les différentes modalités à inclure dans cette politique, la Directive impose également le recours à des processus formels de sécurité de l'information permettant d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

1. OBJECTIFS

La présente politique a pour objectifs de permettre au Cégep :

- de 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 comporte des renseignements personnels;
- d'orienter et de déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information de l'institution défini plus bas dans cette politique.

2. DÉFINITIONS[1]

- **Document** : un ensemble constitué d'informations portées par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrits sous l'une de ces formes ou en un autre système de symboles. Est assimilée au document toute banque de données dont les

[1] Ces définitions proviennent des documents listés à la section 3 de la présente politique

éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

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

- **Responsable d'actifs informationnels** : le membre du personnel cadre détenant la plus haute autorité au sein d'une unité pédagogique ou administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité. Aux fins de l'application de la présente politique, il peut s'agir d'un autre membre du personnel-cadre de l'unité désigné par la personne qui détient la plus haute autorité au sein de l'unité.

- **Détenteur** : une personne qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels du Cégep.

- **Détenteur de l'information** : un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau-cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent.

- **Sécurité de l'information** : la protection de l'information et des systèmes d'information contre les risques et les incidents.

- **Cadre de gestion** : l'ensemble des consignes qu'elles soient les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues qui encadrent les activités d'un établissement qu'est un Cégep.

- **Registre d'incident** : un recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, les mesures prises pour le rétablissement à la normale et le suivi.

- **Registre d'autorité** : le répertoire, le recueil ou le fichier dans lequel sont notamment consignées les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information ainsi que les responsabilités qui y sont rattachées.

- **Confidentialité** : la propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

- **Renseignement confidentiel** : un renseignement, une 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 et la vérification.

- **Renseignement personnel** : une 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, un renseignement personnel aux fins de la présente politique.

- **Accès ou autorisation** : l'attribution par le Cégep à une personne ou à un groupe de personnes d'un droit d'accès, complet ou restreint, à une information ou à un système d'information.

- **Incident** : un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

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

- **CERT/AQ** : le Computer Emergency Response Team/Administration Québécoise, une appellation reconnue internationalement pour les équipes spécialisées en gestion des incidents de sécurité, qui assiste les ministères et les organismes en réduisant les délais d'intervention lors des incidents et en les informant des vulnérabilités et des nouvelles menaces.

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

- **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 qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

- **Système d'information** : l'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

- **Utilisatrice ou utilisateur** : toute personne qui, dans le cadre de ses fonctions, conserve l'information que le Cégep détient dans l'accomplissement de sa mission, ainsi que les ressources qui la sous-tendent ou toute personne physique, appartenant ou non à la communauté collégiale, autorisée à accéder à une information appartenant au Cégep ou sous la responsabilité du Cégep au moyen de l'un de ses systèmes d'information. Les membres du

personnel du Cégep ainsi que les étudiants sont les premiers utilisateurs de l'information du Cégep.

- **Qualités de la sécurité d'une information** (peu importe la forme du document) :

  - *Confidentialité* : la propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.
  - *Disponibilité* : la propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.
  - *Intégrité* : la propriété d'une information de ne 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.
  - *Authentification* : permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif.
  - *Imputabilité* : le principe selon lequel une violation ou une tentative de violation d'un système informatique est attribuée à l'entité qui en est responsable (non-répudiation).
  - *Traçabilité* : la capacité d'associer une action à une identité.

- **Catégorisation**: le 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.

- **Cycle de vie de l'information**: l'ensemble des étapes que franchit l'information, de sa création 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 Cégep.

- **Mesure de sécurité de l'information** : un moyen concret assurant partiellement ou totalement la protection d'information du Cégep 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.

- **Plan de continuité** : l'ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité du Cégep.

- **Plan de relève** : le plan de reprise hors site mis en œuvre lorsqu'il y a détérioration ou destruction d'actifs informationnels consécutive à un incident exigeant le transfert de l'exploitation dans un autre lieu. Le plan de relève décrit les procédures visant à assurer, dans des conditions de continuité adaptées aux critères de survie du Cégep, la mise à la disposition rapide et ordonnée des moyens de secours ainsi que la reprise éventuelle de l'exploitation normale après réfection ou remplacement des actifs détruits ou endommagés.

- **Technologie de l'information** : tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

3. 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 (Décret no 261-2012 du 28 mars 2012);
- la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- le Cadre gouvernemental de gestion de la sécurité de l'information;
- 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 (Décret 7-2014 du 15 janvier 2014);
- la Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- le Code d'éthique du Cégep Limoilou relatif à l'utilisation des technologies de l'information (C-05);
- la Directive du Cégep Limoilou portant sur l'usage de l'Infonuagique publique (C-06).

4. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à tout le personnel, 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.

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. Cette information est composée de renseignements personnels d'étudiants et de membres du personnel, d'information professionnelle sujette à des droits de propriétés intellectuelles (enseignants et chercheurs) et, finalement, d'information stratégique ou opérationnelle pour l'administration du Cégep.

Tous les supports, incluant le papier, sont concernés.

5. PRINCIPES DIRECTEURS

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

a) Par la mise à jour d'un inventaire d'actifs informationnels, s'assurer de bien connaitre l'information à protéger et ses caractéristiques de sécurité en plus d'identifier les personnes responsables.

b) 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.

c) Adhérer à une approche basée sur le risque acceptable. 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.

d) 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 et suffisante en nombre. Cette équipe doit définir, mettre en place, opérer et ajuster la gestion de la sécurité de l'information.

e) Protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle.

f) Reconnaître que l'environnement technologique est en changement constant et interconnecté avec le monde, ce qui impose la mise en place d'une gestion de la sécurité de l'information qui s'adapte à ces changements.

g) 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.

h) 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.

i) Adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de sécurité de l'information avec les réseaux de l'éducation et des organismes publics;

j) Adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle, chaque individu ayant accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci.

k) S'assurer que chaque employé ait accès au minimum d'information requis pour accomplir ses tâches normales.

l) Communiquer de façon transparente au sujet des menaces pouvant affecter les actifs informationnels afin que chacun puisse comprendre l'importance d'appliquer la sécurité requise et être informé de telle sorte qu'il puisse reconnaître les incidents de sécurité et agir en conséquence.

m) Mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels à la clientèle, selon un temps prévu.

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 permettant, notamment, une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être remises en question de manière périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces et des risques.

La présente 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.

6.1. Gestion des accès

La gestion des accès doit être encadrée et contrôlée afin que la divulgation et l'utilisation de l'information soient strictement réservées aux personnes autorisées. Ces mesures ont pour objectif de protéger l'intégrité et la confidentialité des données ainsi que 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 de personnel du Cégep.

6.2. 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 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 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 doivent être déclarés conformément à la Directive sur la sécurité de l'information gouvernementale.

Le niveau de protection de l'information est établi en fonction :

- de la nature de l'information et de son importance;
- des probabilités d'accident, d'erreur ou de malveillance auxquels elle est exposée;
- des conséquences de la matérialisation de ces risques;
- du niveau de risque acceptable par le Cégep.

6.3. Gestion des incidents

Le Cégep déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires pour :

- limiter l'occurrence des incidents en matière de sécurité de l'information;
- gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés conformément à la Directive sur la sécurité de l'information gouvernementale.

7. 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.

7.1. Conseil d'administration

Le conseil d'administration adopte la Politique sur la sécurité de l'information ainsi que toute modification à celle-ci.

7.2. Directeur général

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.

7.3. Responsable de la sécurité de l'information (RSI)

La fonction du responsable de la sécurité de l'information (RSI) est déléguée à un cadre par le conseil d'administration. 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. Plus spécifiquement, le RSI :

- élabore et propose le programme de sécurité de l'information du Cégep et rend compte de son implantation au comité de direction;
- 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 Cégep en matière de sécurité de l'information en conseillant les responsables d'actifs informationnels;
- produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information;
- propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de services et les contrats;
- s'assure de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- collabore à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille au déploiement de ceux-ci;
- procède aux enquêtes dans des transgressions sérieuses ayant trait, selon toute vraisemblance, à la politique, avec l'autorisation du directeur général;
- 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.

7.4. Coordonnateur sectoriel de la gestion des incidents (CSGI)

Le coordonnateur sectoriel de la gestion des incidents représente le Cégep en matière de déclaration des incidents à portée gouvernementale. Le responsable de la sécurité de l'information (RSI) désigne les personnes agissant à titre de CSGI au Cégep. Ces derniers ont la responsabilité :

- de participer activement au réseau d'alerte gouvernementale;
- d'assurer le relais entre le Cégep et le CERT/AQ et de mettre en œuvre les stratégies de réaction appropriées;
- de déclarer les incidents au CERT/AQ;
- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information au Cégep;
- de contribuer aux analyses de risques de sécurité de l'information, d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
- de seconder le RSI.

7.5. Secrétaire général

En sa qualité de responsable des archives, de l'accès aux documents et de la protection des renseignements personnels, le secrétaire général agit comme personne-ressource pour toute question ou problématique relative à la sécurité des renseignements personnels détenus par le Cégep. Il veille à l'établissement des mesures de protection des renseignements personnels à l'égard des documents, à l'application de telles mesures et à ce que des correctifs soient apportés le cas échéant.

7.6. Responsable d'actifs informationnels

Le responsable d'actifs informationnels est le directeur ou la directrice d'une direction. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de cette direction. Le responsable d'actifs informationnels peut déléguer la totalité ou bien une partie de sa responsabilité à un autre des cadres de sa direction.

Le responsable d'actifs informationnels :

- informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de la Politique sur la sécurité de l'information et des dispositions du Cadre de gestion de la sécurité de l'information 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 sur la sécurité de l'information et de tout autre élément du Cadre de gestion;
- s'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité;
- rapporte à la Direction des systèmes et des technologies de l'information (DSTI) toute menace ou tout incident afférant à la sécurité de l'information numérique;
- collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'information;
- rapporte au RSI tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

7.7. Direction des systèmes et des technologies de l'information (DSTI)

En matière de sécurité de l'information, la DSTI s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels elle intervient. Cette direction :

- 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;
- 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 des services d'un système d'information faisant appel aux technologies de l'information 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.

7.8. Direction des services administratifs

- Contribue à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep;
- Sécurise et contrôle les accès physiques aux locaux du Cégep.

7.9. Direction des ressources humaines

- Informe la DSTI d'une embauche, d'un changement de fonction et de fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels du Cégep;
- Informe tout nouvel employé de ses obligations découlant de la présente politique et obtient son engagement à la respecter.

7.10. Personnel d'encadrement

- S'assure que le personnel placé sous sa responsabilité est au fait de ses obligations découlant de la présente politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information;
- Communique à la DSTI tout problème d'importance en matière de sécurité de l'information.

7.11. Utilisateur des actifs informationnels du Cégep

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

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

À cette fin, l'utilisateur doit :

- se conformer à la présente politique et à toute autre directive du Cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- participer à la catégorisation de l'information de son service;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration, ni les désactiver;

- signaler au responsable des actifs informationnels de son service tout incident susceptible de constituer une contravention à la présente politique ou 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 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 lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

8. SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, tout le personnel du Cégep doit être sensibilisé :

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

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement.

9. 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 ne soit 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 tel que défini dans l'article 9 du Code d'éthique relatif à l'utilisation des technologies de l'information (C-05).

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.

10. ENTRÉE EN VIGUEUR ET RÉVISION DE LA POLITIQUE

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration. Le Cégep procède à l'examen de la politique et de sa révision lorsque l'évolution du cadre juridique, social ou technologique le commande.