Cégep de Drummondville

Direction des études

POLITIQUE N^{O} 11

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Adoptée le 5 mai 2020

Adoptée au conseil d'administration
Politique de gestion des documents administratifs :
14 juin 2005 (CA-05-06-14-19)

Politique sur la sécurité de l'information :
5 mai 2020 (CA-20-05-05-14)

960, rue Saint-Georges
Drummondville (Québec) J2C 6A2
www.cegepdrummond.ca

819.478.4671
info@cegepdrummond.ca

TABLE DES MATIÈRES

PRÉAMBULE

Étant donné que l'information est une ressource stratégique de l'organisation, il importe donc d'organiser efficacement l'information produite ou reçue, d'en planifier la durée de vie et, enfin, d'en assurer la protection et l'accessibilité. Cette politique permet au Cégep de Drummondville 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 et dont la conservation est assurée par lui-même ou par un tiers. Cette information est multiple et diversifiée. Elle consiste en des renseignements personnels d'étudiantes et d'étudiants et de membres du personnel, en de l'information professionnelle sujette à des droits de propriétés intellectuelles (personnel enseignant et chercheuses et chercheurs) et, finalement, en de l'information stratégique ou opérationnelle pour l'administration du cégep, en format numérique et même papier.

Dans ce contexte, l'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03) et de la *directive sur la sécurité de l'information gouvernementale* (une directive du Conseil du trésor du Québec applicable au cégep) 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 – dont les principales modalités sont définies dans la directive gouvernementale – en ayant recours, notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des accès, la gestion des documents administratifs, la gestion des risques et la gestion des incidents.

Tous les documents administratifs appartiennent au cégep, tout en demeurant sujets à des droits de propriétés intellectuelles (personnel enseignant et chercheurs et chercheuses) et tout employé, au moment de son départ, doit s'assurer de remettre à son successeur ou à son supérieur, selon le cas, tous les documents relatifs à son travail qu'il a en sa possession, peu importe le support.

Tous les documents administratifs du cégep sont regroupés selon le Plan de classification des documents administratifs du cégep et conservés selon les règles du calendrier de conservation des documents approuvées par Bibliothèque et Archives nationales du Québec (BAnQ) en 1990 et ses mises à jour subséquentes.

L'ensemble des règles énoncées dans la présente politique s'applique aux documents conservés sous un modèle de gestion intégrée des documents (GID).

1. 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 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, l'authenticité et la fiabilité de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

Par conséquent, le cégep met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information de l'institution.

Le cadre de gestion de la sécurité de l'information renforce les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins du cégep en matière de réduction du risque associé à la protection de l'information.

2. 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);
- Bibliothèque et Archives nationales du Québec (BAnQ);
- 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);
- la politique relative à l'utilisation des technologies de l'information et des communications;

3. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisatrices et aux utilisateurs de l'information, c'est-à-dire 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 qui 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.

Tous les supports, incluant le papier, sont concernés.

4. PRINCIPES DIRECTEURS

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

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

4.2 d'assurer une gestion effective et efficace des documents par un meilleur contrôle de la création/réception, de la classification, du classement, de la diffusion, de l'utilisation, de l'exploitation, de la protection et du repérage des documents;

4.3 reconnaître l'importance de la politique de sécurité de l'information, du cadre de gestion de la sécurité de l'information qui doit être articulé par une équipe compétente (cette équipe devant définir, mettre en place, opérer et ajuster la gestion de la sécurité de l'information);

4.4 protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle en considérant qu'ils servent uniquement aux fins desquels ils ont été recueillis;

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

4.6 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 de recouvrement des activités compromises;

4.7 mettre en place un plan de relève du collège en cas de sinistres majeurs.

4.8 protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction (le niveau de sécurité pouvant varier au cours du cycle de vie du document) en adoptant de bonnes pratiques en matière de gestion documentaire;

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

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

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

5. DÉFINITIONS

« **Document confidentiel** » : tout document qui contient une information de nature confidentielle ou privilégiée, ou traitée de cette façon par le Cégep de Drummondville, et ce, peu importe sa forme ou le support technique utilisé. Cette information comprend, de manière non limitative, tous les renseignements personnels ainsi que les renseignements d'ordre administratifs, financiers, scientifiques, techniques ou commerciaux créés, collectés, utilisés, ou conservés dans le cadre des activités du Cégep de Drummondville.

« **Renseignement personnel** » : tout renseignement qui concerne une personne physique et permet de l'identifier (article 54 Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels), tel qu'une adresse, un numéro de téléphone, une note d'examen, un numéro d'assurance sociale ou un matricule.

6. CADRE DE GESTION

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

Le cadre de gestion vise à renforcer les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et des directives gouvernementales, ainsi qu'aux autres besoins du Collège en matière de réduction du risque associé à la protection de l'information. Le cadre de gestion consiste en un ensemble de directives, de règles et de procédures permettant au Collège de s'acquitter des contrôles nécessaires en matière de protection de l'information.

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 politique de sécurité de l'information du cégep s'articule autour de trois axes fondamentaux de gestion. Ces axes sont la gestion des accès, la gestion des risques et la gestion des incidents.

6.1 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 quant à l'utilisation des actifs informationnels, à tous les niveaux de personnel du cégep.

6.2 Gestion des documents administratifs

L'adoption par l'Assemblée nationale de la *Loi sur les archives* et de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, de même que les coûts élevés de traitement de ressources documentaires entraînent la nécessité d'établir une gestion rigoureuse des documents administratifs.

Des outils de gestion documentaire présentent les principales règles relatives à la classification, à la conservation, à l'utilisation et à la consultation des documents administratifs dont le Cégep a la responsabilité.

Une bonne gestion des documents administratifs se traduira par une réduction des documents conservés dans les services, une meilleure protection des documents à valeur historique et un repérage plus rapide de la documentation utilisée fréquemment tout en permettant également :

- de préciser le rôle de chacun des intervenants;
- d'éviter la multiplication excessive des documents;
- de diminuer la masse de documents à conserver tout en préservant ceux qui ont une valeur administrative, légale, fiscale ou historique;
- de rationaliser l'utilisation de l'espace et des équipements de classement des documents tant physique que numérique.

6.3 Gestion des risques

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du cégep. La gestion des risques liés à la sécurité de l'information s'inscrit dans le

processus global de gestion des risques du cégep. Les risques à portée gouvernementale sont déclarés conformément à la directive sur la sécurité de l'information gouvernementale.

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

- 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.

6.4 Gestion des incidents

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

- 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 (par le CERT/AQ).

Dans la gestion des incidents, le cégep peut exercer ses pouvoirs et ses prérogatives en égard à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

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 de sécurité de l'information ainsi que toute modification à celle-ci. Le conseil est informé des actions du cégep en matière de sécurité de l'information. Il est le dirigeant de l'organisme responsable de l'application de la politique en sécurité de l'information.

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

7.2 Régie de direction

La régie de direction du cégep détermine des mesures visant à favoriser l'application de la politique et des obligations légales du cégep en matière de sécurité de l'information. Ainsi, elle détermine les orientations stratégiques, les plans d'action et les bilans de sécurité de l'information. Elle peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

7.3 Direction générale

La direction générale veille à l'application de la politique sur la sécurité de l'information.

Ses tâches seront les suivantes :

- d'encadrer la ou le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat;
- de déléguer certaines responsabilités à la ou au secrétaire général pour la gestion de l'information;
- de faire adopter par le conseil d'administration les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information;
- d'autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission du cégep;
- d'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique;

7.4 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 de la directrice ou 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. Cette personne est nommée par le conseil d'administration.

Le RSI :

- élabore et propose le programme de sécurité de l'information du cégep, 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 dans les services;
- produit les plans d'action, tient un registre des incidents, 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 service 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 présumément à la politique à la suite de l'autorisation de la directrice générale ou du directeur général du collège;
- 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.

7.5 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. C'est un comité temporaire qui est plutôt tactique et opérationnel.
Ce comité est chargé en particulier de mettre en place le cadre de gestion, les plans d'action et les bilans de sécurité de l'information, les activités de sensibilisation ou de formation ainsi que toutes propositions d'action en matière de sécurité de l'information. C'est aussi un forum d'échange entre les parties prenantes ou d'observation de l'évolution du projet en sécurité de l'information.

Le comité sera formé des parties prenantes du cégep qui seront directement concernées ou qui participent au projet de mise en place de la sécurité de l'information.

- La direction des études;
- La coordination du service intégré des technologies de l'information ;
- Le secrétariat général ;
- La direction aux ressources humaines ;
- Le professionnel responsable de la gestion documentaire

7.6 Service des technologies de l'information

En matière de sécurité 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;
- 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, 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 la directrice ou le directeur général.

7.7 Service des ressources matérielles

Le service des ressources matérielles participe, avec le RSI, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du cégep.

7.8 Secrétariat général

Le secrétariat général tient à jour le registre des dérogations et le registre des cas de contravention à la présente politique.

7.9 Service des ressources humaines

En matière de sécurité de l'information, le service des ressources humaines obtient de toute nouvelle employée ou de tout nouvel employé du cégep, après lui en avoir montré la nécessité, son engagement au respect de la politique.

Le service des ressources humaines informe le service des technologies de l'information de toute embauche, tout changement de statut et tout départ d'employée ou d'employé. Il vérifie les antécédents pour les personnels en lien avec des données sensibles.

7.10 Bureau de gestion documentaire

Le bureau de gestion documentaire :

- élabore les politiques, normes, procédures et méthodes de travail liées à la gestion des documents;

- est responsable de l’élaboration et de l’application d’un système de classification uniforme pour l’ensemble des documents actifs du cégep;
- est responsable de l’application des règles de conservation définitives des dossiers;
- coordonne et supervise les activités liées à l’implantation du système de classification uniforme dans les différents services;
- supporte les services à tout moment dans les différentes étapes de la chaîne documentaire;
- assure la protection particulière des documents essentiels du cégep (lettres patentes, règlements, budgets, titres de propriété, baux, assurances, procès-verbaux, etc.);
- assure le suivi dans le système informatique des différents éléments liés à la gestion des documents et des procès-verbaux; concernant ces derniers, un système de repérage informatisé permet l’accès à l’information contenue dans les procès-verbaux du conseil d’administration, du comité exécutif et de la commission des études.

7.11 Responsables d’actifs informationnels

La ou le responsable d’actifs informationnels est le cadre détenant l’autorité au sein d’un service, qu'elle soit d’ordre pédagogique ou d’ordre administratif, et dont le rôle consiste à veiller à l’accessibilité, à l’utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il peut donc y avoir plusieurs responsables d’actifs informationnels dans un cégep. La ou le responsable d’actifs informationnels peut déléguer la totalité ou bien une partie de sa responsabilité à une ou un autre membre du service.

La ou le responsable d’actifs informationnels :

- informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de la politique de sécurité de l’information et des dispositions du cadre de gestion 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 soient prises en compte dans tout processus d’acquisition et tout contrat de service sous sa responsabilité et voit à ce que tout consultant ou consultante, fournisseur, partenaire, invité ou invitée, organisme ou firme externe s’engage à respecter la politique et tout autre élément du cadre de gestion;
- 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;

- rapporte à la directrice générale ou au 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.

Les services sont responsables de leurs dossiers jusqu'à l'archivage définitif des dossiers.

7.12 Utilisateurs

La responsabilité de la sécurité de l'information du cégep incombe à toutes les utilisatrices et à tous les utilisateurs des actifs informationnels du cégep.

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 qu'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 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 à la ou au responsable des actifs informationnels de son service tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du cégep;
- 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, toute utilisatrice ou tout utilisateur du cégep doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

8. SENSIBILISATION ET INFORMATION

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

- à l'importance des opérations de gestion documentaire;
- 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 en fonction du plan de perfectionnement élaboré par la Direction des ressources humaines. De plus, des documents explicatifs sont disponibles sur le site Internet du cégep.

9. SANCTIONS

En cas de contravention à la présente politique, l’utilisatrice ou 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 (dont celles des conventions collectives de travail et du Règlement relatif aux règles du milieu de vie collégial du collège).

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, une ou un partenaire, une ou un invité, une consultante ou 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. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le RSI, assisté du comité de travail pour la sécurité de l’information, est responsable de la diffusion et de la mise à jour de la politique. La politique de sécurité de l’information sera révisée au plus tard cinq ans après son adoption.

11. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil d’administration, soit le 5 mai 2020.