



POL-15 Politique sur la sécurité de l'information

Adoptée par le Conseil d'administration le 25 septembre 2017.



POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION¹

TABLE DES MATIÈRES

Article 1	PRÉAMBULE	3
Article 2	DÉFINITIONS	3
Article 3	OBJECTIFS	4
Article 4	CADRE LÉGAL ET ADMINISTRATIF	5
Article 5	CHAMP D'APPLICATION	5
Article 6	PRINCIPES DIRECTEURS	6
Article 7	CADRE DE GESTION	6
	7.1 Gestion des accès	7
	7.2 Gestion des risques	7
	7.3 Gestion des incidents	7
Article 8	RÔLES ET RESPONSABILITÉS	8
	8.1 Conseil d'administration	8
	8.2 Directeur général	8
	8.3 Direction générale	8
	8.4 Responsable de la sécurité de l'information (RSI)	8
	8.5 Direction des technologies informatiques	9
	8.6 Direction des finances et des ressources matérielles	9
	8.7 Direction des ressources humaines	9
	8.8 Responsable d'actifs informationnels	10
	8.9 Utilisateurs	10
Article 9	SENSIBILISATION ET INFORMATION	11
Article 10	SANCTIONS	11
Article 11	DIFFUSION ET MISE À JOUR DE LA POLITIQUE	12
Article 12	ENTRÉE EN VIGUEUR	12

¹ Dans ce document, l'utilisation du masculin pour désigner des personnes a comme seul but d'alléger le texte et identifie sans discrimination les individus des deux sexes.

Article 1 PRÉAMBULE

Cette politique permet au Cégep Garneau 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 il est le gardien.

Cette information est multiple et diversifiée : renseignements personnels d'étudiants et de membres du personnel, information professionnelle sujette à des droits de propriété intellectuelle (professeurs et chercheurs), information stratégique ou opérationnelle pour l'administration du Cégep.

L'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale* crée des obligations aux établissements 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 sur la 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.

Article 2 DÉFINITIONS

a) « 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 media 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.

b) « 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.

c) « 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.

d) « 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.

- e) « 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.
- f) « 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.
- g) « 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.

Article 3 OBJECTIFS

La présente Politique a pour objectif d'affirmer l'engagement du Cégep à s'acquitter de ses obligations à l'égard de la sécurité de l'information, quel que soit 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 constitue des renseignements personnels.

Par conséquent, le Cégep se dote d'une politique visant à orienter et à déterminer sa vision qui sera détaillée par le cadre de gestion de la sécurité de l'information de l'institution.

Ce cadre 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.

Article 4 CADRE LÉGAL ET ADMINISTRATIF

La *Politique sur la sécurité de l'information* s'inscrit dans un contexte légal principalement constitué de:

- la *Charte des droits et libertés de la personne* (RLRQ, c. C-12);
- le *Code civil du Québec*;
- le *Code criminel* ;
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) et ses règlements;
- la *Directive sur la sécurité de l'information gouvernementale*;
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) et ses règlements;
- la *Loi sur les archives* (RLRQ, c. A-21.1);
- la *Loi sur le droit d'auteur* (RLRC, 1985, c. C-42).

Dans le cadre administratif du Cégep :

Le *Règlement sur la protection des renseignements personnels* (R-07);

Le *Règlement concernant la gestion des documents administratifs et des archives* (R-11);

Le *Code de conduite des utilisateurs des actifs informatiques*.

Article 5 CHAMP D'APPLICATION

La présente *Politique* s'applique aux utilisateurs de l'information : tout le personnel, toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou d'invité utilise les actifs informationnels du Cégep.

L'information visée est celle que le Cégep détient dans le cadre de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

Tous les supports d'information, incluant le papier, sont concernés.

Article 6 PRINCIPES DIRECTEURS

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

1. identifier l'information à protéger, ses caractéristiques de sécurité et désigner les personnes qui en sont responsables;
2. 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;
3. adhérer à une approche basée sur le risque acceptable;
4. protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle jusqu'à sa destruction éventuelle;
5. mettre en place une gestion de la sécurité de l'information qui répond au changement constant de l'environnement technologique;
6. évaluer régulièrement les risques, mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, définir des actions d'éradication des menaces ou de recouvrement des activités compromises;
7. adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de sécurité de l'information avec le réseau de l'éducation et les organismes publics;
8. adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle;
9. s'assurer que chaque employé ait accès à seule l'information pertinente pour la réalisation de ses tâches normales;
10. s'assurer d'une communication efficace dans les situations pouvant affecter les actifs informationnels et être identifiées comme des menaces;
11. mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels.

Article 7 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.

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 sur la 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;
- la gestion des incidents;

7.1 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 et sur l'imputabilité des personnes, à tous les niveaux de personnel du Cégep.

7.2 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 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.

7.3 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 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*.

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 8 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.

8.1 Conseil d'administration

Le Conseil d'administration adopte la *Politique sur la sécurité de l'information* ainsi que toute modification à celle-ci. Le Conseil d'administration nomme le Responsable de la sécurité de l'information (RSI) tel que requis par la Loi. Il est informé des actions du Cégep en matière de sécurité de l'information.

8.2 Directeur général

Le directeur général est responsable de l'application de la *Politique sur la sécurité de l'information*.

- Il autorise, 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;
- Il autorise une enquête lorsqu'il y a ou pourrait y avoir transgression de la Politique.

8.3 Direction générale

La direction générale du Cégep adopte 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 reçoit les bilans de sécurité de l'information.

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

Le RSI est nommé par le Conseil d'administration. Il relève du directeur général au sens du *Cadre gouvernemental de gestion de la sécurité de l'information*. Cette personne :

- élabore et propose le cadre de gestion de la sécurité de l'information du Cégep et rend compte de son implantation à la Direction générale;
- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les règles et les bonnes pratiques en matière de sécurité de l'information et propose des mises à jour de 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 unités;
- 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 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 relatives à des transgressions réelles ou présumées ayant trait à la Politique, à la suite de l'autorisation du directeur général;
- tient à jour le registre des dérogations et le registre des cas de contravention à la présente Politique;
- 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.

8.5 Direction des technologies informatiques

En matière de sécurité de l'information, la Direction des technologies informatiques 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 :

- 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 faisant appel aux technologies de l'information;
- elle applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information;
- elle participe à l'exécution des enquêtes informatiques relatives à des contraventions réelles ou apparentes à la présente Politique, autorisées par le directeur général.

8.6 Direction des finances et des ressources matérielles

La Direction des finances et des ressources matérielles, avec le responsable de la sécurité de l'information, voit à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

8.7 Direction des ressources humaines

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

8.8 Responsable d'actifs informationnels

Le responsable d'actifs informationnels est le gestionnaire 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. Le responsable d'actifs informationnels peut déléguer une partie de sa responsabilité à un autre gestionnaire du service.

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 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 autorisé 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 services sous sa responsabilité et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la Politique et tout autre élément du cadre de gestion;
- rapporte à la Direction des technologies informatiques 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 au RSI tout problème lié à l'application de la présente Politique, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de cette Politique.

8.9 Utilisateurs

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;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- signaler au responsable du service ou du département, 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 atténuer une menace à la sécurité de l'information ou à un incident de sécurité de l'information.

Aussi, tout utilisateur du Cégep doit se conformer aux politiques et aux directives en vigueur au Cégep 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.

Article 9 SENSIBILISATION ET INFORMATION

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

- 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. De plus, des documents explicatifs sont disponibles sur le site Internet du Cégep.

Article 10 SANCTIONS

En cas de contravention à la présente Politique, l'utilisateur engage sa responsabilité personnelle; il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente Politique et aux mesures de sécurité de l'information qui en découlent, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles disciplinaires internes applicables.

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 11 DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le RSI, assisté par la Direction des communications et des affaires corporatives, est responsable de la diffusion et de la mise à jour de la Politique.

La Politique sur la sécurité de l'information est révisée et modifiée au besoin.

Article 12 ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur dès son adoption par le Conseil d'administration et remplace la *Politique de sécurité sur les technologies de l'information et des télécommunications*.



R-07 Règlement sur la protection des renseignements personnels

Adopté par le Conseil d'administration le 28 octobre 2002.



RÈGLEMENT SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS¹

TABLE DES MATIERES

1.	DÉFINITION DES TERMES	1
2.	RÈGLE D'INTERPRÉTATION.....	2
3.	CHAMP D'APPLICATION	2
4.	RESPONSABILITÉS	2
5.	PRINCIPES	
	5.1 Possession de renseignements nominatifs	3
	5.2 Propriété des renseignements nominatifs	3
	5.3 Caractère confidentiel des renseignements nominatifs.....	3
6.	RÈGLES GÉNÉRALES	
	6.1 Collecte de renseignements nominatifs	3
	6.2 Constitution d'un dossier de renseignements nominatifs	4
	6.3 Responsable de dossier	4
	6.4 Droit d'accès aux renseignements nominatifs	4
	6.5 Exercice du droit d'accès	4
	6.6 Mesures de sécurité.....	5
	6.7 Transmission de renseignements nominatifs	5
	6.8 Étalage et affichage.....	5
	6.9 Usage du télécopieur.....	6
	6.10 Transmission informatique	6
	6.11 Archivage des renseignements nominatifs	6
	6.12 Destruction des renseignements confidentiels.....	6
	6.13 Entreposage temporaire	6
7.	RÈGLES PARTICULIÈRES	
	7.1 Information à l'étudiant	7
	7.2 Contenu du dossier.....	7
	7.3 Gestion du dossier.....	7
	7.4 Droit d'accès au dossier	7
	7.5 Information au personnel	8
	7.6 Contenu du dossier.....	9
	7.7 Gestion du dossier.....	9
	7.8 Droit d'accès au dossier	9
	7.9 Information au client.....	10
	7.10 Contenu du dossier.....	10
	7.11 Gestion du dossier.....	10
	7.12 Droit d'accès au dossier	11
8.	DATE D'ENTRÉE EN VIGUEUR	11

¹ Dans ce document, l'utilisation du masculin pour désigner des personnes a comme seul but d'alléger le texte et identifie sans discrimination les individus des deux sexes.

1. DÉFINITION DES TERMES

Dans le présent règlement, les termes suivants signifient :

- a) « RENSEIGNEMENT NOMINATIF » :
dans un document, sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier. Les renseignements nominatifs sont confidentiels.
- b) « ÉTUDIANT » :
la personne admise au Cégep dans un programme d'études collégiales et inscrite à un ou des cours de ce programme ou inscrite à une formation sur mesure.
- c) « PERSONNEL » :
personne à l'emploi ou ayant été à l'emploi du Cégep, comme régulier ou occasionnel, incluant les personnes chargées de cours, de projets ou activités spécifiques contractuelles, dans quelque catégorie que ce soit, syndiquée ou non.
- d) « CLIENT » :
une personne qui, sur une base volontaire, participe aux activités offertes par une unité (par exemple : les clients des cliniques de santé, du centre d'activités physiques)
- e) « DOSSIER PRINCIPAL » :
le dossier officiel d'une personne contenant l'ensemble des renseignements nominatifs nécessaires à la gestion de son statut (étudiant, membre du personnel, client) au Cégep ou de sa participation à un service ou à un programme.
- f) « DOSSIER SECONDAIRE » :
le dossier contenant copie, en tout ou en partie, des renseignements versés au dossier principal ainsi que les pièces nécessaires à la gestion courante d'un programme et dont l'usage est restreint à des fins internes à une unité.
- g) « DOSSIER PHYSIQUE » :
dossier manuel ou mécanique qui comprend des renseignements nominatifs et qui constitue un dossier principal ou secondaire.
- h) « DOSSIER INFORMATIQUE » :
dossier informatisé qui comprend des renseignements nominatifs et qui constitue un dossier principal ou secondaire.
- i) « UNITÉ » :
toute composante administrative du Cégep, soit un service administratif ou un département.
- j) « RESPONSABLE D'UNITÉ » :
la personne détenant la plus haute autorité au sein d'une unité ou, le cas échéant, la personne à laquelle le responsable délègue la responsabilité en matière d'application du présent règlement dans son unité.

- k) « CALENDRIER DE CONSERVATION » :
outil de gestion documentaire élaboré pour fixer les règles de conservation des différents types de documents du Cégep, compte tenu de leur valeur administrative, légale ou historique en application de la Loi sur les archives.
- l) « LOI » :
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

2. RÈGLE D'INTERPRÉTATION

- 2.1** En cas de difficulté d'interprétation du présent règlement, le Cégep convient de s'en référer au texte de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* [L.R.Q., chap. A-2.1].
- 2.2** Certaines pratiques visent à limiter davantage l'accès à un dossier comprenant des renseignements personnels que ne le prévoit le présent Règlement; celui-ci ne peut avoir comme effet de rendre ces pratiques moins restrictives.

3. CHAMP D'APPLICATION

Le présent règlement s'applique à l'ensemble des unités du Cégep et à toute personne qui, dans l'exercice de ses fonctions au Cégep, recueille, consulte ou possède des renseignements nominatifs.

4. RESPONSABILITÉS

- 4.1** Le secrétaire général, nommé « responsable de la protection des renseignements personnels » par le directeur général en vertu de l'article 8 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, voit, pour et au nom du Cégep, à la mise en œuvre et au respect du présent règlement. Aux seules fins de l'exercice de ses responsabilités eu égard à l'application de ladite loi, le secrétaire général ou un membre de son personnel affecté à ces fins a accès à tout dossier qui comprend des renseignements nominatifs. Les avis du secrétaire général sont prescriptifs et il a le pouvoir de vérifier et inspecter tout processus ou dossier en lien avec l'application de la Loi ou du présent règlement.
- 4.2** En concertation avec le secrétaire général, toute personne occupant un poste de responsable d'unité voit à l'application de la Loi et du présent règlement dans les opérations de son unité; il soumet une procédure au secrétaire général en matière de collecte, de communication de renseignements personnels et de déclarations de dossiers de renseignements personnels.

- 4.3** Un comité consultatif exerce un rôle conseil auprès du secrétaire général; il participe à l'élaboration d'un plan d'action en matière d'accès à l'information et de protection de renseignements personnels, notamment en ce qui a lien à la formation des membres du personnel; il exerce une veille notamment en validant les nouveaux projets de collecte de renseignements personnels et les projets visant à développer et implanter une technologie susceptible d'affecter la protection des renseignements personnels.

5. PRINCIPES

5.1 Possession de renseignements nominatifs

Le Cégep possède des renseignements nominatifs sur les personnes dans les seuls cas où cela s'avère indispensable à l'exercice de ses attributions ou à la mise en œuvre d'un programme ou d'une activité s'inscrivant dans sa mission.

5.2 Propriété des renseignements nominatifs

Le Cégep est propriétaire des renseignements nominatifs et des dossiers qu'il détient sur les personnes.

5.3 Caractère confidentiel des renseignements nominatifs

Le Cégep reconnaît que les renseignements nominatifs qu'il possède sur les personnes ont un caractère confidentiel.

6. RÈGLES GÉNÉRALES

6.1 Collecte de renseignements nominatifs

Lorsque le Cégep entend constituer un dossier comprenant des renseignements nominatifs, il doit, au moment où il recueille de tels renseignements pour une première fois auprès d'une personne :

- s'identifier;
- indiquer clairement l'usage qu'il entend faire des renseignements qu'il conservera;
- préciser les catégories de personnes qui auront accès à ces renseignements.

Il doit en outre aviser cette même personne :

- du caractère obligatoire ou facultatif des demandes de renseignements qui lui sont formulées ainsi que des conséquences d'un refus de communiquer ces renseignements;
- de son droit d'accéder aux renseignements recueillis et de les rectifier.

(Voir les *Règles particulières* aux articles 7.1, 7.5 et 7.9)

Par la même occasion, le Cégep sollicite, le cas échéant, le consentement de la personne concernée à la transmission de certains renseignements nominatifs à des tiers à des fins précises jugées conformes à son intérêt et au rôle du Cégep.

6.2 Constitution d'un dossier de renseignements nominatifs

Toute unité qui constitue un dossier de renseignements nominatifs en fait la déclaration au secrétaire général. De même, toute modification importante quant au contenu du dossier ou quant aux fins pour lesquelles il existe est soumise au secrétaire général pour approbation.

6.3 Responsable de dossier

Le responsable d'un dossier principal ou secondaire est le responsable de l'unité qui possède un tel dossier.

6.4 Droit d'accès aux renseignements nominatifs

6.4.1 Le Cégep veille à ce que l'accès à un dossier contenant des renseignements nominatifs soit réservé à la seule personne concernée et aux personnes dûment autorisées par cette dernière ou par le présent règlement.

6.4.2 Tout renseignement nominatif que possède le Cégep qu'il soit inclus ou non dans un dossier de renseignements nominatifs, fait l'objet, *mutatis mutandis*, de la protection accordée en vertu du présent règlement.

6.4.3 Toute personne qui souhaite avoir accès aux renseignements nominatifs que possède le Cégep et qui n'y est pas autorisée en vertu du présent règlement doit, pour ce faire, s'adresser par écrit au secrétaire général.

6.5 Exercice du droit d'accès

6.5.1 Toute personne dûment autorisée par le présent règlement à avoir accès à un dossier ou à recevoir un renseignement nominatif conservé dans un dossier doit exercer la vigilance nécessaire pour éviter que des personnes non autorisées y aient accès.

6.5.2 Toute personne a le droit, après s'être dûment identifiée, de prendre connaissance des renseignements nominatifs la concernant, là où ces renseignements sont conservés, pendant les heures de bureau du Cégep, après entente avec l'autorité compétente et en présence de cette dernière ou d'une personne déléguée par celle-ci. Elle peut également en obtenir communication sous la forme d'une transcription écrite.

6.5.3 Une personne qui a accès à son dossier personnel ne peut consulter en même temps un avis ou une recommandation faite par un membre du Cégep dans l'exercice de ses fonctions ou par un tiers qui, sans être membre du Cégep, a accepté, au su de la personne en cause ou à la demande du Cégep de produire un avis ou une recommandation à son endroit, tant que la décision finale n'a pas été prise.

6.6 Mesures de sécurité

6.6.1 Afin d'assurer le caractère confidentiel des dossiers comprenant des renseignements nominatifs, chacune des unités qui possède de tels dossiers voit à l'instauration de mesures de sécurité et ce, tant pour les dossiers physiques qu'informatiques.

6.6.2 Chacune des unités qui possède des dossiers comprenant des renseignements nominatifs informe le secrétaire général des mesures de sécurité qu'elle a adoptées et l'avise de toute modification qui y est apportée.

6.7 Transmission de renseignements nominatifs

6.7.1 Sous réserve des dispositions du présent règlement relatives au droit d'accès aux renseignements nominatifs que possède le Cégep, la transmission de tels renseignements exige le consentement de la personne concernée.

6.7.2 Le Cégep peut cependant transmettre un renseignement nominatif à une personne ou à un organisme sans le consentement de la personne concernée lorsque cette transmission est nécessaire à l'application d'une loi, à l'application d'une convention collective ou d'un règlement qui établit les relations de travail ou à l'exercice d'un mandat de gestion administrative dont l'exécution est confiée par le Cégep à cette personne ou à cet organisme.

6.7.3 Dans tous les cas où il peut s'avérer indispensable de transférer des renseignements nominatifs à une autre personne ou organisme et que les dispositions prévues aux articles précédents (cf. art. 6.7.1 et 6.7.2) ne peuvent s'appliquer, le Cégep peut conclure une entente de transfert sous la responsabilité du secrétaire général.

6.7.4 Le secrétaire général est responsable de la tenue du registre conformément aux règles établies par la Commission d'accès à l'information et la Loi.

6.8 Étalage et affichage

Aucun élément versé ou destiné à être versé dans un dossier de renseignements nominatifs ne doit faire l'objet d'affichage ou d'étalage. On peut cependant afficher des éléments d'un dossier de renseignements nominatifs à la condition que l'identification de la personne en cause ne soit possible que par elle-même et se limite à l'affichage de son numéro matricule ou de tout autre signe ou symbole propre à celle-ci.

6.9 Usage du télécopieur

Lorsqu'il s'agit de transmettre des renseignements confidentiels, les modes de transmission qui assurent la plus grande confidentialité doivent être privilégiés. L'usage du télécopieur ne devrait être limité aux seules situations qui l'exigent. La lettre d'accompagnement doit signaler la qualité confidentielle du document et doit être effectuée à un poste de réception sûr.

6.10 Transmission informatique

Toute transmission informatique de renseignements confidentiels doit être faite de manière sécuritaire; des dispositifs de sécurité reconnus seront appliqués pour les services personnels offerts sur le Web. L'utilisation du courrier électronique pour la transmission d'information ou de document comprenant des renseignements confidentiels doit être limitée aux seules situations qui l'exigent. Ces messages doivent être détruits dans les délais prescrits.

6.11 Archivage des renseignements nominatifs

Sous réserve de la *Loi sur les archives* ainsi que des politiques de conservation en vigueur au Cégep, les renseignements que possède une unité sont détruits lorsque les fins pour lesquelles ils ont été recueillis ont été atteintes. Aux seules fins de l'exercice de ses responsabilités eu égard à l'application de ladite loi et desdites politiques, le secrétaire général ou un membre de son personnel affecté au secteur des archives a accès à tout dossier comprenant des renseignements nominatifs.

6.12 Destruction des renseignements confidentiels

Tous les documents détenus par le Cégep dans l'exercice de ses fonctions, peu importe leur forme écrite, graphique, sonore, visuelle, informatisée ou autre, qui contiennent des renseignements nominatifs, doivent être détruits sous réserve de la Loi sur les Archives, lorsqu'ils sont périmés. Ils sont déchiquetés, effacés, déchirés de façon à ce que l'on ne puisse en reconstituer le contenu.

Les documents, brouillons, notes personnelles contenant des renseignements nominatifs doivent être détruits de manière à les rendre illisibles; les disquettes, disques, cartouches et rubans magnétiques qui contiennent des renseignements nominatifs doivent être complètement effacés ou rendus illisibles avant d'être jetés.

6.13 Entreposage temporaire

Lorsque les documents contenant des renseignements nominatifs ne peuvent être détruits ou déchiquetés sur place, ils doivent être entreposés temporairement dans un endroit verrouillé.

Lorsque des documents confidentiels sont regroupés dans des boîtes, on y appose la mention « documents confidentiels à détruire ». Elles doivent être toujours conservées dans des locaux fermés à clef.

Le Secrétaire général du Cégep est responsable de l'entreposage temporaire des documents confidentiels à détruire de même que de l'expédition de ces documents vers un point central de destruction et de la supervision de cette destruction.

7. RÈGLES PARTICULIÈRES

A) Le dossier de l'étudiant

7.1 Information à l'étudiant

Le Cégep indique à tout étudiant, lors du dépôt de la demande d'admission, l'usage qu'il entend faire des renseignements nominatifs qu'il versera à son dossier et précise les catégories de personnes qui auront accès à ces renseignements (cf. art. 6.1).

7.2 Contenu du dossier

Le contenu du dossier de l'étudiant est décrit dans le Calendrier de conservation des documents du Cégep.

7.3 Gestion du dossier

7.3.1 Le dossier principal de l'étudiant inscrit à l'enseignement régulier est géré par le Service des ressources à l'enseignement.

7.3.2 Le dossier principal de l'étudiant inscrit à la formation continue est géré par le Service de la formation continue.

7.3.3 Les dossiers secondaires sont gérés, aux fins pédagogiques, par les responsables d'unité, et, aux fins de l'administration financière, par le Service des finances et de la paie.

7.4 Droit d'accès au dossier

7.4.1 Les personnes suivantes ont accès, sans restriction, au dossier :

- a) de l'étudiant de toutes catégories
 - les cadres supérieurs, les adjoints au directeur des études et le secrétaire général ainsi que, lorsque requis dans l'exercice de ses fonctions, un membre de la direction, d'un service pédagogique ou du bureau du secrétaire général;
- b) de l'étudiant de toutes catégories dans la juridiction du responsable du dossier
 - un membre du personnel dont la fonction est d'assister immédiatement un responsable ayant accès au dossier;
 - un membre du personnel affecté à la gestion du dossier;

- c) de l'étudiant inscrit à un programme dispensé au Service de la formation continue
 - le directeur du Service de la formation continue et ses adjoints.

7.4.2 Les personnes suivantes sont autorisées à obtenir les seuls renseignements nécessaires à l'exercice de leurs fonctions, telles qu'elles sont définies dans les règlements des études ou qui s'inscrivent dans le mandat de leur unité :

- un membre du personnel enseignant, aux seules fins de la réalisation de ses tâches, notamment la prestation de cours, de laboratoires, de stages et pour l'encadrement des étudiantes et étudiants;
- les membres d'un comité d'admission ou d'appel en matière d'admission;
- les membres d'un comité de discipline ou d'un comité d'appel en matière de discipline;
- le directeur et le personnel autorisé* du Service des finances et de la paie;
- le directeur et le personnel autorisé* du Service de l'informatique;
- le directeur et le personnel autorisé* du Centre des médias;
- le directeur du Service des affaires étudiantes et communautaires et le personnel autorisé* des composantes de cette unité;
- le responsable d'une activité parascolaire pour les étudiants inscrits à cette activité.

7.4.3 Une personne ayant un droit d'accès partiel au dossier en vertu de l'article 7.4.2 peut, sur autorisation expresse du responsable du dossier, avoir accès à des renseignements autres que ceux auxquels lui donne droit ledit article, à la condition qu'elle fournisse une justification de sa demande, fondée sur l'exercice de ses fonctions, et qu'elle démontre, à la satisfaction du responsable, qu'on doit présumer du consentement de la personne en cause. Tout accès consenti en vertu du présent article fait l'objet d'un enregistrement versé au dossier.

B) Le dossier du personnel

7.5 Information au personnel

Le Cégep indique à toute personne qu'il embauche, l'usage qu'il entend faire des renseignements nominatifs qu'il versera à son dossier et précise les catégories de personnes qui auront accès à ces renseignements (cf. art. 6.1).

* Le secrétaire général, après entente avec le responsable de l'unité, détermine les catégories de personnes autorisées en vertu du présent règlement.

7.6 Contenu du dossier

Le dossier d'un membre du personnel est constitué de tous les documents et renseignements nécessaires à sa gestion et, notamment, ceux qui sont requis par les conventions collectives, protocoles ou contrats de travail le concernant de même que les documents et renseignements requis pour l'application des lois, des régimes de retraite et des assurances collectives.

Est également considéré comme dossier l'ensemble des curriculum vitae reçus pour offres de services.

7.7 Gestion du dossier

7.7.1 Le dossier principal :

- a) du personnel de toutes les catégories sauf le personnel occupant un poste de cadre est géré par le Service des ressources humaines;
- b) du personnel occupant un poste de cadre est géré par la Direction générale.

7.7.2 Les dossiers secondaires sont gérés dans les unités de rattachement des membres du personnel à des fins internes et au Service des finances et de la paie aux fins de la gestion financière.

7.8 Droit d'accès au dossier

7.8.1 Les personnes suivantes ont accès, sans restriction, au dossier :

- a) du personnel de toutes catégories
 - le directeur général, le directeur du Service des ressources humaines ainsi que, lorsque requis dans l'exercice de ses fonctions, un membre de la Direction générale ou du Service des ressources humaines;
 - le responsable d'une unité pour le personnel qui lui est rattaché;

Toutefois, les coordonnateurs de département n'ont pas accès au dossier du personnel de leur unité.

- b) du personnel de toutes catégories dans la juridiction du responsable du dossier
 - un membre du personnel dont la fonction est d'assister immédiatement un responsable ayant accès au dossier;
 - un membre du personnel affecté à la gestion du dossier;
- c) du personnel enseignant
 - le directeur des études et ses adjoints pour les enseignants du secteur régulier;
 - le directeur du Service de la formation continue et ses adjoints pour les enseignants du secteur de la formation continue.

Cas particulier relatifs à l'évaluation du personnel

Nonobstant ce qui précède :

- seul le directeur des études peut avoir accès aux pièces relatives à l'évaluation faite en vertu de la Politique sur l'évaluation du personnel enseignant;
- seul le supérieur immédiat d'un cadre et le directeur général peuvent avoir accès à l'évaluation de celui-ci faite en vertu de la Politique d'évaluation du personnel cadre.

7.8.2 Les personnes suivantes sont autorisées à obtenir les seuls renseignements nécessaires à l'exercice de leurs fonctions en ce qui a trait au personnel :

a) de toutes catégories

- le directeur et le personnel autorisé* du Service des finances et de la paie;
- le directeur et le personnel autorisé* du Service de l'informatique;
- le directeur et le personnel autorisé* du Centre des médias.

C) Le dossier du client

7.9 Information au client

Le Cégep indique à tout client, lors de son inscription à une activité, l'usage qu'il entend faire des renseignements nominatifs qu'il versera à son dossier et il précise les catégories de personnes qui auront accès à ces renseignements (cf. art. 6.1).

7.10 Contenu du dossier

Le contenu du dossier de chaque client est établi en fonction de la nature et des fins particulières de chacune des unités qui offre des services.

7.11 Gestion du dossier

7.11.1 Le dossier principal de chaque client du Cégep est géré par l'unité qui lui offre des services.

7.11.2 Selon la nature des activités de l'unité, un dossier secondaire peut être consulté au Service des finances à des fins de gestion financière.

* Le secrétaire général, après entente avec le responsable de l'unité, détermine les catégories de personnes autorisées en vertu du présent règlement.

7.12 Droit d'accès au dossier

7.12.1 Sous réserve de l'application de l'article 7.12.3, les personnes suivantes ont accès au dossier du client inscrit à un programme offert par un service collectif :

- le responsable et le personnel autorisé* de l'unité qui offre un service collectif.

7.12.2 Sous réserve de l'application de l'article 7.12.3, les personnes suivantes sont autorisées à obtenir les seuls renseignements nécessaires à l'exercice de leurs fonctions eu égard aux services collectifs :

- le directeur général;
- le directeur et le personnel autorisé* du Service des finances et de la paie;
- le directeur et le personnel autorisé* du Service de l'informatique.

7.12.3 Nonobstant les articles 7.12.1 et 7.12.2, seules les personnes suivantes ont accès au dossier complet de leur propre client :

- le personnel d'une unité qui offre un service individuel dans le cadre de règles précises prescrites par un code de déontologie et le personnel de soutien directement affecté au traitement des dossiers de ces professionnels;
- les étudiants d'un programme où les activités d'enseignement et d'apprentissage le nécessitent, ceci sous la supervision du professeur du cours.

8. DATE D'ENTRÉE EN VIGUEUR

Le présent règlement entre en vigueur dès son adoption.

* Le secrétaire général, après entente avec le responsable de l'unité, détermine les catégories de personnes autorisées en vertu du présent règlement.

R-07 Règlement sur la protection des renseignements personnels

Date d'entrée en vigueur de la première version du Règlement : Le 28 octobre 2002

Dates de modification :