

COLLÈGE D'ENSEIGNEMENT GÉNÉRAL
ET PROFESSIONNEL
BEAUCE-APPALACHES

Politique de sécurité de l'information

Table des matières

PRÉAMBULE	3
Article 1 – Définitions	3
Article 2 - Cadre légal et institutionnel	4
Article 3 – Principes généraux	4
Article 4 - Objectifs	4
Article 5 - Champs d'application	5
5.1 - Personnes visées	5
5.2 - Actifs visés	5
5.3 - Activités visées	5
Article 6 - Dispositions générales et particulières	5
6.1 - Gestion des identités et des accès	6
6.2 – Gestion des vulnérabilités	6
6.3 - Gestion des risques	6
6.4 - Gestion des incidents	6
6.5 – Gestion de reprise et de continuité des activités	7
6.6 – Protection des locaux et du matériel	7
6.7- Sensibilisation et information	7
6.8 - Droit de regard	7
Article 7 - Responsabilités	7
7.1 Conseil d'administration	7
7.2 Directeur général	7
7.3 Responsable de la protection des renseignements personnels	8
7.4 Chef de la sécurité de l'information organisationnelle (CSIO)	8
7.5 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)	8
7.6 Direction des ressources informationnelles	8
7.7 Service des ressources matérielles, volet Sécurité et protection	8
7.8 Direction des ressources humaines	9
7.9 Détenteur d'actifs informationnels	9
7.10 Utilisateurs	9
Article 8 – Contravention à la politique	10
Article 9 - Date d'entrée en vigueur	10
Article 10 - Évaluation et révision	10
ANNEXE 1 – Fondements légaux	11

PRÉAMBULE

Le Cégep Beauce-Appalaches reconnaît que l'information est essentielle à ses opérations courantes et qu'elle doit donc faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. Il reconnaît détenir, en outre, des renseignements personnels ainsi que des informations qui ont une valeur légale, administrative ou économique. Plusieurs lois et directives encadrent et régissent l'utilisation de l'information. Le Cégep Beauce-Appalaches est assujéti à ces lois et doit s'assurer du respect de celles-ci.

La présente Politique de sécurité de l'information fournit donc aux usagers et usagères les repères nécessaires afin qu'ils puissent utiliser les ressources informationnelles du Cégep en respect des lois encadrant l'accès à l'information de façon à préserver la réputation de l'organisation et à la protéger des risques inhérents au monde de la technologie.

Article 1 – Définitions

Actif informationnel : Une information, une banque d'information, un système ou un support d'information, une documentation, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par le Cégep Beauce-Appalaches.

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.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information : Ensemble des étapes que franchit une information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation du Cégep Beauce-Appalaches.

Détenteur-trice d'actif informationnel : Cadre à qui est assignée la responsabilité de la sécurité d'un actif informationnel.

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

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.

Information : Un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Intégrité : Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

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.

Personne utilisatrice : Une ou un membre du personnel du Cégep, un·e contractant·e, un·e étudiant·e ou un·e client·e ayant accès à l'actif informationnel du Cégep.

Article 2 - Cadre légal et institutionnel

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales. Pour plus de précisions, voir l'Annexe 1.

De plus, le Cégep a adopté le règlement suivant :

- *Règlement relatif à la protection et la sécurité des personnes et des biens du Cégep Beauce-Appalaches.*

Article 3 – Principes généraux

Le Cégep adhère au cadre gouvernemental québécois en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

Il reconnaît que les actifs informationnels qu'il détient sont essentiels à ses opérations courantes et, de ce fait, doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Leur niveau de protection est établi en fonction de leur importance, de leur confidentialité et des risques d'accidents, d'erreurs et de malveillance auxquels ils sont exposés.

Les mesures de protection, de prévention, de détection, d'assurance et de correction doivent permettre d'assurer la confidentialité, l'intégrité, la disponibilité, l'accessibilité et l'irrévocabilité des actifs informationnels de même que la continuité des activités.

Le Cégep Beauce-Appalaches s'engage à sensibiliser et à former son personnel à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en cette matière.

Article 4 - Objectifs

La présente politique vise à assurer le respect par le Cégep Beauce-Appalaches de toute obligation opérationnelle et de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et des télécommunications.

Plus spécifiquement, les objectifs en matière de sécurité de l'information sont :

- Assurer l'intégrité, l'irrévocabilité, la disponibilité, la confidentialité, le contrôle d'accès, la surveillance et l'administration à l'égard de l'utilisation des réseaux informatiques, des télécommunications et d'Internet, de l'utilisation des actifs informationnels et des données corporatives ;
- Identifier les actifs informationnels du Cégep et s'assurer de leur évaluation constante, de leur utilisation appropriée et de leur protection adéquate ;
- Identifier, réduire et contrôler les risques pouvant porter atteinte aux informations ou aux systèmes d'informations du Cégep ou de ses clientèles ;

- Assurer le respect de la vie privée des individus, notamment, la confidentialité des renseignements à caractère nominatif relatifs à la communauté étudiante, au personnel du Cégep et aux partenaires d'affaires provenant du milieu des affaires ou de l'industrie ;
- Assurer la conformité aux lois et règlements applicables ;
- Établir un plan de continuité et de relève des services informatiques du Cégep ;
- Sensibiliser et former les personnes visées à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

Article 5 - Champs d'application

La présente politique en matière de sécurité de l'information ainsi que les directives et procédures sous-jacentes et les règles qui leur sont associées s'appliquent aux personnes, aux activités et aux actifs suivants :

5.1 - Personnes visées

Cette politique s'adresse à toute la communauté étudiante, à tout le personnel œuvrant au Cégep Beauce-Appalaches sans égard à son statut et aux membres du conseil d'administration. De plus, elle s'étend à toute personne dûment autorisée qui utilise ou qui accède dans l'exercice de ses fonctions pour le compte du Cégep, à des informations confidentielles ou non. Les consultant·e·s, partenaires et fournisseurs·euses utilisant et ayant accès aux biens du Cégep ou ayant des biens du Cégep sous leur garde, sont aussi visés par cette politique.

5.2 - Actifs visés

Cette politique s'applique à l'ensemble des actifs informationnels ainsi qu'à leur utilisation au sein du Cégep, tels que les bases de données sans égard aux médiums de support (fixe ou portable), les réseaux, les systèmes d'information, les logiciels, les équipements informatiques utilisés par l'établissement, que ces actifs fassent partie de l'une ou l'autre des trois catégories suivantes :

- Appartenant au Cégep et exploités par l'organisation ;
- Appartenant au Cégep et exploités ou détenus par un·e fournisseur·euse de services ou un·e tiers·ce.
- Appartenant à un·e fournisseur·euse de services ou un·e tiers·ce et exploités par celui-ci au profit du Cégep. Dans ce cas-ci, le fournisseur doit respecter l'esprit de la présente politique.

5.3 - Activités visées

Cette politique concerne l'ensemble des activités composant le cycle de vie de l'information sous toutes ses formes à savoir : la définition, la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation (archivage, sauvegarde et récupération), et la destruction (mise au rebut) des actifs informationnels du Cégep, que ces activités soient conduites dans ses locaux, dans un autre lieu ou à distance.

Article 6 - Dispositions générales et particulières

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différentes personnes utilisatrices 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.

6.1 - Gestion des identités et des accès

La gestion des identités et 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.

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée ou illicite. Sont notamment considérés comme confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences néfastes, notamment sur les relations intergouvernementales, les négociations entre organismes, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

6.2 – Gestion des vulnérabilités

La gestion des vulnérabilités se caractérise par un déploiement des mesures pour maintenir à jour les logiciels du parc informatique, afin de garder les vulnérabilités au niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une gestion de notification des vulnérabilités venant des fournisseur-euses ou des prestataires de services doit être en place pour qu'elles soient évaluées et corrigées, le cas échéant.

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.

Les actifs informationnels doivent faire l'objet d'une identification et d'une classification. Le niveau de protection de chaque actif informationnel doit être identifié par la personne détentrice en fonction de sa criticité, de sa sensibilité et des risques d'accidents, d'erreurs et de malveillance auxquels elle est exposée.

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'accidents, d'erreurs 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 :

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

À cet égard, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels du Cégep est assuré.

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

6.5 – Gestion de reprise et de continuité des activités

Le Cégep Beauce-Appalaches prévoit un mécanisme de relève des composantes critiques pour assurer la prestation des services jugés prioritaires lors d'une panne informatique ou technique.

6.6 – Protection des locaux et du matériel

Tous les accès physiques à des locaux comportant des actifs informationnels appartenant au Cégep doivent être contrôlés afin d'empêcher tout dommage ou toute intrusion. Des mécanismes appropriés de contrôle d'accès doivent être mis en place à l'entrée des locaux en fonction des risques identifiés.

Tout support d'information emmagasinant les données sensibles doit faire l'objet d'une surveillance continue et de mesures de contrôle appropriées selon son degré de criticité afin de le préserver de tout dommage.

6.7- Sensibilisation et information

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle.

À cet égard, le personnel et les membres du conseil d'administration du Cégep doivent être sensibilisés :

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

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. De plus, des documents explicatifs sont disponibles sur le portail du Cégep.

6.8 - Droit de regard

Comme les actifs informationnels appartiennent au Cégep, celui-ci a un droit de regard sur l'utilisation qui en est faite par une personne utilisatrice. Les circonstances pour lesquelles ce droit de regard peut être exercé doivent être clairement définies et diffusées auprès des personnes utilisatrices.

Article 7 - 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'ils 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. Il est régulièrement 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 de sécurité de l'information.

7.2 Direction générale

La direction générale fait 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. Elle assume aussi le processus de délégation des rôles de CSIO et COMSI.

7.3 Responsable de la protection des renseignements personnels

La personne responsable de la protection des renseignements personnels veille à assurer le respect et la mise en œuvre de la Loi sur la protection des renseignements personnels afin de mettre en œuvre des politiques et pratiques encadrant la gouvernance des renseignements personnels.

7.4 Chef de la sécurité de l'information organisationnelle (CSIO)

La personne assumant la fonction de CSIO est membre du personnel d'encadrement. Ce ou cette chef assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. La fonction de CSIO est déléguée par la direction générale.

Le ou la CSIO est responsable de la diffusion et de la mise en application de la politique.

7.5 Fonction de coordonnateur-trice organisationnel-le des mesures de sécurité de l'information (COMSI)

La personne assumant la fonction de COMSI agit sur le plan opérationnel. Elle intervient dans la mise en œuvre des mesures et apporte le soutien nécessaire au responsable de la protection des renseignements personnels ou à la personne occupant la fonction de CSIO de l'établissement, notamment en matière de la gestion des incidents et des risques en sécurité de l'information.

Le ou la COMSI représente le Cégep auprès du Réseau d'alerte gouvernemental. Il ou elle est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI), en soutien à la personne jouant le rôle de chef de la sécurité de l'information organisationnelle (CSIO).

Il ou elle collabore auprès du ou de la CSIO du Cégep à l'élaboration des divers éléments stratégiques et tactiques en sécurité informationnelle :

- Maintient le registre des événements et des incidents liés à la sécurité de l'information;
- Effectue et participe aux analyses de risques en sécurité de l'information;
- Gère le processus de gestion, de déclaration des incidents et de résolution de problème et contribue à sa mise en place;
- Contribue au processus formel de gestion des droits d'accès à l'information.

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 dans lesquels il intervient :

- Il 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;
- Il applique des mesures de réaction appropriées à toute menace et à tout incident de sécurité de l'information, tels que par exemple l'interruption ou la révocation temporaire - lorsque les circonstances l'exigent - des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause;
- Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la direction générale.

7.7 Service des ressources matérielles, volet Sécurité et protection

- Le service des ressources matérielles, volet Sécurité et protection procède aux enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la direction générale;
- Il participe, avec le ou la coordonnateur-trice organisationnel-le des mesures de sécurité de l'information (COMSI), à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

7.8 Service des ressources humaines

En matière de sécurité de l'information, le service des ressources humaines doit :

- Vérifier, au besoin, les antécédents des personnes à l'embauche et des membres du personnel impliqués dans la sécurité de l'information;
- S'assurer que les responsabilités des intervenant·e·s concernant la sécurité de l'information et le respect de la présente politique, ainsi que du cadre normatif des ressources informationnelles, sont inscrites dans les descriptions de tâches des membres du personnel;
- Informer et obtenir de toute nouvelle personne embauchée Cégep son engagement au respect de la présente politique;
- Imposer les sanctions appropriées lors de violation des politiques, règlements, directives et code de conduite touchant à la sécurité de l'information.

7.9 Détenteur·trice d'actifs informationnels

Le personnel d'encadrement est le détenteur d'actifs informationnels dans son champ de responsabilités. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous sa responsabilité. Il peut donc y avoir plusieurs détenteur·trice·s d'actifs informationnels au Cégep. Le ou la détenteur·trice d'actifs informationnels peut déléguer la totalité ou bien une partie de sa responsabilité à une autre personne du service.

Le ou la détenteur·trice d'actifs informationnels :

- Informe le personnel relevant de son autorité et les tierces personnes 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 sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voit à ce que tout consultant·e, fournisseur·euse, partenaire, invité, 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 au ou à la Chef de la sécurité de l'information organisationnelle toutes contraventions ou tous problèmes liés à l'application de la présente politique, dont toute contravention réelle ou apparente d'un·e membre du personnel à ce qui a trait à l'application de cette politique.

7.10 Personnes utilisatrices

La responsabilité de la sécurité de l'information du Cégep incombe à toutes les personnes utilisatrices des actifs informationnels du Cégep. À cet effet, un message portant sur la confidentialité de l'information est affiché lors du démarrage d'un équipement informatique du Cégep.

Toute personne utilisatrice 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, la personne utilisatrice 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 pour les 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 ne modifier leur configuration, ni ne les désactiver;
- Signaler au détenteur ou à la détentrice d'actifs informationnels de son unité 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 personne utilisatrice du Cégep doit se conformer aux politiques, procédures et aux directives en vigueur dans une entreprise ou un organisme avec lequel elle est en relation dans le cadre de ses activités professionnelles ou d'études lorsqu'il y a partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

Article 8 – Contravention à la politique

En cas de contravention à la présente politique, la personne utilisatrice 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.

Un ou une 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. Ces mesures peuvent inclure la suspension des privilèges d'accès, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur.euse, 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

La Direction générale décide de l'application de l'une ou l'autre, ou plusieurs de ces sanctions. Elle peut également transmettre à toute autorité judiciaire les informations colligées sur toute personne utilisatrice d'actifs informationnels ayant contrevenu à cette politique et qui portent à croire qu'une infraction à l'une ou l'autre loi ou règlement en vigueur a été commise. Le ou la contrevenant.e doit alors faire face à des mesures légales et s'expose à des poursuites judiciaires.

Article 9 - Date d'entrée en vigueur

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

Article 10 - Évaluation et révision

Afin d'assurer son adéquation aux besoins de sécurité du Cégep et s'ajuster aux nouvelles pratiques et technologies utilisées, la présente politique est révisée lors de tout changement important qui pourrait l'affecter.

Toute modification à la présente politique doit être sanctionnée par le conseil d'administration du Cégep sur recommandation de la direction générale

ANNEXE 1 – Fondements légaux

- La Directive gouvernementale sur la sécurité de l'information;
[Directive gouvernementale sur la sécurité de l'information](#)
- Cadre gouvernemental de gestion de la sécurité de l'information
[Cadre gouvernemental de gestion de la sécurité de l'information](#)
- Aide-mémoire : Politique gouvernementale en cybersécurité
[Politique gouvernementale en Cybersécurité - Mesures Clés](#)
- La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
[Loi concernant le cadre juridique des technologies de l'information](#)
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1);
[Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#)
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25);
[Aide-Mémoire: Modernisation de la protection des renseignements personnels | Gouvernement du Québec](#)
- Règlement sur les incidents de confidentialité
[Règlement sur les incidents de confidentialité](#)
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03);
[Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement](#)
- Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la *Loi sur la gouvernance et la gestion des ressources informationnelles*;
[Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la LGGRI](#)
- Règles relatives à la gestion des projets en ressources informationnelles;
[Règles relatives à la gestion des projets en ressources informationnelles](#)
- Règles relatives à la planification et à la gestion des ressources informationnelles;
[Règles relatives à la planification et à la gestion des ressources informationnelles](#)
- La *Loi sur les archives* (LRQ, chapitre A-21.1);
[Loi sur les archives](#)
- Les lois sectorielles régissant la mission de chaque organisme;

- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2);
[Règlement sur la diffusion de l'information et sur la protection des renseignements personnels](#)
- La Charte des droits et libertés de la personne (LRQ, chapitre C-12);
[Charte des droits et libertés de la personne](#)
- Le Code civil du Québec (LQ, 1991, chapitre 64);
[Code civil du Québec](#)
- Le Code criminel (LRC, 1985, chapitre C-46);
[Code criminel](#)
- Loi sur la fonction publique (RLRQ, chapitre F-3.1.1);
[Loi sur la fonction publique](#)
- Toute autre loi ou règle applicable.

Fondements normatifs :

- Le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;
- Le cadre gouvernemental de gestion de la sécurité de l'information;
- Les normes internationales, notamment ISO 27000 et NIST 800-60;
- Les pratiques gouvernementales en matière de sécurité de l'information.