CÉGEP
BEAUCE-APPALACHES

COLLÈGE D'ENSEIGNEMENT GÉNÉRAL
ET PROFESSIONNEL
BEAUCE-APPALACHES

Politique de sécurité de l'information

1055, 116e Rue
(Québec) G5Y 3G1
: : www.cegepba.qc.ca

La présente politique a été adoptée
par le conseil d'administration
le 6 février 1997
Révisée le 11 décembre 2017

Table des matières

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 assujetti à ces lois et doit s'assurer du respect de celles-ci.

La présente Politique de sécurité de l'information fournit donc aux usagers les repères nécessaires afin qu'ils puissent utiliser les ressources informationnelles du Cegep 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 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.

Utilisateur : Un membre du personnel du Cégep, un contractant, un étudiant ou un client ayant accès à l'actif informationnel du Cegep.

Article 2 - Cadre légal et institutionnel

La Politique de sécurité de l'information s'inscrit principalement dans un contexte régi par :

- *La Charte des droits et libertés de la personne (LRQ, chapitre C-12);*
- *Le Code civil du Québec (LQ, 1991, chapitre 64);*
- *La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;*
- *La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);*
- *La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);*
- *La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);*
- *La Loi sur les archives (LRQ, chapitre A-21.1);*
- *Le Code criminel (LRC, 1985, chapitre C-46);*
- *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);*
- *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 clientèle étudiante, au personnel du Cégep et à tout partenaire 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 tous les étudiants, à tout le personnel œuvrant au Cégep Beauce-Appalaches sans égard à son statut et aux administrateurs. 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 consultants, partenaires et fournisseurs 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 fournisseur de services ou un tiers.
- Appartenant à un fournisseur de services ou un tiers 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.

5.4 - Comité sur la sécurité de l'information

Le comité sur la sécurité de l'information relève du responsable de la sécurité de l'information (RSI) et constitue un mécanisme de coordination et de concertation qui, par sa vision globale, est en mesure de proposer des orientations et de faire des recommandations à la direction générale et au conseil d'administration.

Ce comité propose et met 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.

Il est également en mesure d'évaluer les incidences sur la sécurité de l'organisation que les nouveaux projets pourraient avoir. Il approuve les standards, les pratiques et le plan d'action de sécurité de l'information du Cégep et met en application les mesures d'audit approuvées. Exceptionnellement, si la situation exige une action immédiate, il prend les mesures nécessaires, qu'il fait entériner dans les meilleurs délais.

Le comité sur la sécurité de l'information est constitué :

- Du responsable de la sécurité de l'information (RSI) ;
- Du coordonnateur sectoriel de la gestion des incidents (CSGI) ;
- Du responsable de la prévention et de la sécurité.

Périodiquement, le comité sur la sécurité de l'information doit réviser le Registre des incidents et s'assurer que toutes les solutions qui ont été appliquées sont encore effectives et valables à la date de la révision.

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 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.

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.

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 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 son détenteur en fonction de sa criticité, de sa sensibilité et des risques d'accidents, d'erreurs et de malveillance auxquels il est exposé.

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.

6.3 - 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 :

- 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 eu égard à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

6.4 – 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.

6.5 – 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.

6.6- Sensibilisation et information

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les employés 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.

6.7 - 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 un utilisateur. Les circonstances pour lesquelles ce droit de regard peut être exercé doivent être clairement définies et diffusées auprès des utilisateurs.

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'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. 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 Directeur général

Le directeur général veille à l'application de la Politique de sécurité de l'information. Il doit :

- Encadrer le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat ;
- Déléguer certaines responsabilités au secrétaire général pour la gestion de l'information ;
- 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 ;
- Autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique.

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

Le RSI relève du directeur général au sens du Cadre gouvernemental de gestion de la sécurité de l'information. Cette personne met en place le cadre de gestion de la sécurité de l'information et s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins. Il est nommé par le conseil d'administration. Il a pour fonction :

- De soumettre au dirigeant de son organisation les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la SI de son organisation ;
- De contribuer, avec son CSGI (coordonnateur sectoriel de la gestion des incidents en SI) et le COGI-réseau, à la mise en place d'un processus formel de gestion et de déclaration des incidents, incluant un registre des incidents et d'en assurer la mise en œuvre dans son organisation ;
- De s'assurer de la contribution de son organisation au processus de gestion des risques et des incidents de SI à portée gouvernementale ;
- D'assurer la coordination et la cohérence des actions de la SI menées au sein de son organisation par d'autres acteurs, tels que les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique;
- S'assurer que des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats ;
- Participer aux enquêtes dans des transgressions sérieuses ayant trait à la politique à la suite de l'autorisation de la direction générale ;
- Tenir à jour le registre des dérogations et le registre des cas de contravention à la présente politique;
- D'établir des liens avec les autres RSI de son réseau afin de privilégier le partage d'expertises et d'éléments stratégiques et tactiques à élaborer et à mettre en œuvre.

7.4 Coordonnateur sectoriel de la gestion des incidents (CSGI)

Le CSGI apporte son soutien au RSI du Cégep, notamment en ce qui a trait à la gestion des incidents et des risques en SI. Il est l'interlocuteur officiel du Cégep auprès du CERT/AQ. Pour remplir son rôle, il a comme responsabilités :

- De collaborer auprès du COGI-Réseau et du RSI du Cégep à l'élaboration des divers éléments stratégiques et tactiques en SI tels :
    - ✓ Une politique en SI ;
    - ✓ Un cadre de gestion ;
    - ✓ Un registre d'autorité ;
    - ✓ La catégorisation des actifs ;
    - ✓ Des mesures de sécurité pour les actifs critiques ;
    - ✓ Un processus formel de gestion des risques en SI ;
    - ✓ Un processus formel de gestion des droits d'accès à l'information.

- De participer avec le COGI-réseau au processus gouvernemental de gestion des incidents, et au réseau d'alerte gouvernemental coordonné par le CERT/AQ ;
- D'élaborer et de mettre en œuvre, avec le soutien du COGI-réseau, un processus formel de gestion et de déclaration des incidents de son organisme incluant un registre des incidents de son organisation ;
- De coordonner la gestion des incidents de la SI du Cégep et à portées gouvernementales avec le soutien du COGI-réseau :
    - ✓ Mettre en place, si elle n'est pas existante, une équipe de réponse aux incidents (ERI) au Cégep ;
    - ✓ Avec les membres de l'ERI, développer, mettre en place et tester un plan de réponse aux incidents de sécurité de leur organisme scolaire.
- De contribuer aux analyses des risques de la SI, de définir les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées pour son organisation ;
- De contribuer à l'autoévaluation de la sécurité des systèmes informatiques et des réseaux informatiques du Cégep, notamment par des exercices d'audit de sécurité et des tests d'intrusion aux systèmes jugés à risques ;
- D'élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications mis en place au Cégep ;

7.5 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 le directeur général.

7.6 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 le directeur général ;

- Il participe, avec le responsable de la sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

7.7 Service des ressources humaines

- En matière de sécurité de l'information, le service des ressources humaines obtient de tout nouvel employé du Cégep, après lui en avoir montré la nécessité, son engagement au respect de la politique ;

- Il organise des activités de sensibilisation et des séances de formation au personnel du Cégep face 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.

7.8 Détenteur 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 détenteurs d'actifs informationnels au Cégep. Le détenteur d'actifs informationnels peut déléguer la totalité ou bien une partie de sa responsabilité à un autre membre du service.

Le détenteur 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 sont prises en compte dans tout processus d'acquisition et tout contrat de service 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 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 directeur général toutes contraventions ou tous problèmes liés à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

7.9 Utilisateurs

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

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 pour les fins auxquels 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 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, tout utilisateur du Cégep doit se conformer aux politiques, procédures 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.

Article 8 – Contravention à la politique

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. 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, 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 tout utilisateur 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 contrevenant 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 du directeur général