CollègeAhuntsic

RECUEIL DES
RÈGLES DE GESTION

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

(PO-33)

RECUEIL DES RÈGLES DE GESTION

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

(PO-33)

Adoptée par le Conseil d'administration du 28 novembre 2018

TABLE DES MATIÈRES

Veuillez noter que la forme masculine utilisée dans cette Politique désigne aussi bien les femmes que les hommes. Le genre masculin est utilisé sans aucune discrimination et dans le seul but d'alléger le texte.

POLITIQUE DE SÉCURITÉ DE L'INFORMATION (PO-33)

PRÉAMBULE

Le monde d'aujourd'hui n'a plus de frontières et l'espace numérique est à la merci d'actions frauduleuses : vol d'informations personnelles, cyberintimidation, perte de donnée. Notre Collège et ses systèmes d'information sont donc une cible potentielle.

Cette Politique contribue à l'accomplissement de la mission du Collège, 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 multiple et diversifiée est constituée des renseignements personnels d'étudiants et de membres du personnel, de l'information professionnelle sujette à des droits de propriétés intellectuelles (enseignants et chercheurs) et, finalement, de l'information stratégique ou opérationnelle pour l'administration du Collège. Nous sommes interconnectés avec le monde, dans un environnement technologique en changement constant. Une gestion de la sécurité de l'information qui s'adapte à ces transformations est indispensable.

Dans ce contexte, l'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et de la Directive sur la sécurité de l'information gouvernementale[1] obligent les collèges à adopter, mettre en œuvre, maintenir à jour et assurer l'application d'une politique de sécurité de l'information. La présente Politique s'articule autour de trois composantes : la structure fonctionnelle de la sécurité de l'information, le partage des responsabilités entre les intervenants et les rôles attribués aux comités de coordination et de concertation. Elle s'organise également autour de trois axes fondamentaux de gestion, soit ceux des accès, des risques et des incidents.

ARTICLE 1.00 – ABRÉVIATIONS ET DÉFINITIONS

1.01 Abréviations

a) **CERT/AQ** : Computer Emergency Response Team/Administration québécoise ;
b) **CGN** : Comité de gouvernance numérique ;
c) **COGI** : Coordonnateur organisationnel de gestion des incidents ;
d) **DRM** : Direction des ressources matérielles ;
e) **DTI** : Direction des technologies de l'information ;
f) **RSI** : Responsable de la sécurité de l'information.

[1] Directive du Conseil du trésor du Québec applicable aux cégeps.

1.02 Définitions

Dans cette Politique, les expressions et les termes suivants signifient :

a) **« ACTIFS INFORMATIONNELS »** : Information, système d'information, documentation, matériel informatique, installation ou ensemble de ces éléments, acquis ou constitué par le Collège pour mener à bien sa mission.

b) **« CATÉGORISATION DE L'INFORMATION »** : Processus permettant de déterminer le degré de sensibilité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité des dits actifs du Collège.

c) **« CERT/AQ (Computer Emergency Response Team/Administration québécoise) »** : Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale.

d) **« CONFIDENTIALITÉ »** : Propriété d'une information ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées.

e) **« DISPONIBILITÉ »** : Propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

f) **« IMPUTABILITÉ »** : Principe selon lequel une violation ou une tentative de violation d'un système informatique est attribuée à l'entité qui en est responsable.

g) **« INCIDENT »** : 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.

h) **« INCIDENT DE SÉCURITÉ DE L'INFORMATION À PORTÉE GOUVERNEMENTALE »** : Atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale, nécessitant une intervention concertée.

i) **« INFORMATION »** : Renseignement consigné sur tout support pour être conservé, traité ou communiqué.

j) **« INTÉGRITÉ » :** Propriété d'une information intacte, entière, qui n'a pas été altérée, volontairement ou accidentellement, lors de son traitement ou de sa transmission.

k) **« MESURE DE SÉCURITÉ DE L'INFORMATION »** : Moyen concret assurant partiellement ou totalement la protection des actifs informationnels du Collège contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs institutionnels, acte involontaire, acte malveillant tel que l'intrusion dans un système informatique, etc.) et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

l) **« NIVEAU DE MATURITÉ ADÉQUAT »** : Un niveau de maturité convenable en sécurité de l'information est atteint lorsque les processus de sécurité de l'information et de protection des renseignements personnels et de la vie privée sont normalisés, intégrés, documentés et mis en

œuvre et lorsque l'information gouvernementale est sécurisée, conformément aux meilleures pratiques de sécurité de l'information et en tenant compte des menaces qui pèsent sur celle-ci.

m) **« PLAN DE CONTINUITÉ »** : 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 Collège.

n) **« PLAN DE RELÈVE »** : Plan de reprise hors site mis en œuvre lorsqu'il y a détérioration ou destruction d'actifs informationnels consécutives 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 Collège, 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.

o) **« REGISTRE D'AUTORITÉ »** : Répertoire, recueil ou fichier dans lesquels sont notamment consignées les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information ainsi que les responsabilités qui y sont rattachées.

p) **« REGISTRE D'INCIDENT »** : Recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, son impact, les mesures prises pour le rétablissement à la normale et le suivi.

q) **« RENSEIGNEMENT PERSONNEL »** : Renseignement qui, dans un document, concerne une personne physique et permet de l'identifier, par exemple : le nom, l'adresse, le numéro de téléphone, le statut de fréquentation, le code permanent, le numéro d'employé, la date de naissance, les informations médicales et les numéros de carte de paiement.

r) **« RISQUE ACCEPTABLE »** : Risque dont la conséquence ne met pas en péril ni l'organisation, ni les membres de la communauté.

s) **« RISQUE DE SÉCURITÉ DE L'INFORMATION »** : 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 la protection de leurs renseignements personnels, le respect de leur vie privée, ou sur l'image du Collège.

t) **« RISQUE DE SÉCURITÉ DE L'INFORMATION À PORTÉE GOUVERNEMENTALE »** : Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

u) **« SÉCURITÉ INFORMATIONNELLE »** : Ensemble de mesures de sécurité physiques, informatiques et administratives, et de mesures d'urgence mises en place dans une organisation, en vue d'assurer la protection de l'ensemble de ses actifs informationnels. Plus particulièrement, la sécurité informationnelle assure l'intégrité, la confidentialité, l'authenticité, l'imputabilité, la non-répudiation et la fiabilité des actifs informationnels.

v) **« SYSTÈME D'INFORMATION »** : Système constitué des technologies de l'information, des procédures ainsi que des données qui y sont traitées, et dont le but est de fournir de l'information.

w) **« TECHNOLOGIE DE L'INFORMATION »** : Ensemble du matériel informatique, logiciels, réseau de télécommunication, services technologiques ainsi que les moyens et les méthodes de sécurité informationnelle utilisés pour la collecte, le stockage, le traitement, la transmission, la reproduction, la protection et l'élimination de l'information numérique.

x) **« UTILISATEUR »** : Toute personne physique ou morale utilisant ou ayant accès aux actifs informationnels du Collège. Sont notamment considérés comme des utilisateurs : le personnel enseignant, le personnel professionnel, le personnel de soutien, le personnel-cadre, les étudiants, les organisations syndicales ou associatives qui les représentent, les résidents de la résidence étudiante, les retraités du Collège ainsi que les fournisseurs et les consultants externes.

ARTICLE 2.00 – OBJECTIFS

La présente Politique vise les objectifs suivants :

2.01 Affirmer l'engagement du Collège à s'acquitter pleinement de ses obligations quant à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, le Collège doit veiller à :

a) La disponibilité de l'information de façon qu'elle soit accessible en temps voulu et de manière adéquate aux personnes autorisées ;

b) L'intégrité de l'information de manière que celle-ci ne soit ni détruite ni altérée sans autorisation et que le support de cette information lui procure la stabilité et la pérennité voulues ;

c) La confidentialité de l'information et la protection des renseignements personnels, en limitant l'accès et l'utilisation de ceux-ci aux seules personnes autorisées.

2.02 Orienter et déterminer la vision du Collège en matière de la sécurité de l'information.

2.03 Renforcer les systèmes de contrôles internes en offrant une assurance acceptable de conformité à l'égard des lois et des directives gouvernementales ainsi qu'aux autres besoins du Collège en matière de réduction du risque associé à la protection de l'information.

ARTICLE 3.00 – CADRE JURIDIQUE

La présente Politique est soumise, notamment, aux dispositions suivantes :

a) Le Code criminel (LRC, 1985, chapitre C-46) ;

b) Le Code civil du Québec (LQ, 1991, chapitre 64) ;

c) La Charte des droits et libertés de la personne (LRQ, chapitre C-12) ;

d) La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03) ;

e) La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1) ;

f) La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1) ;

g) La Loi sur les archives (LRQ, chapitre A-21.1) ;

h) La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42) ;

i) La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics ;

j) La Directive sur la sécurité de l'information gouvernementale ;

k) Les Conventions collectives en vigueur au Collège ;

De plus, elle complète les règlements et politiques suivants du Collège ;

l) Politique de gestion intégrée des documents (PO-24) ;

m) Politique sur l'utilisation des technologies de l'information (PO-27) ;

n) Directive sur l'utilisation de l'infonuagique (D-24).

ARTICLE 4.00 – CHAMP D'APPLICATION

4.01 La présente Politique s'adresse à tous les utilisateurs et s'applique à tous les actifs informationnels du Collège.

ARTICLE 5.00 – PRINCIPES DIRECTEURS

5.01 L'efficacité des mesures de sécurité de l'information repose entre autres sur l'attribution de responsabilités et sur l'imputabilité des utilisateurs.

5.02 L'engagement de la Direction ainsi que la collaboration de tous les utilisateurs sont nécessaires à la bonne gestion des risques de sécurité de l'information.

5.03 Sans enfreindre les droits et libertés des membres de la communauté du Collège, la sécurité de l'information requiert la mise en place de mesures proactives, de méthodes de détection d'usage abusif ou inapproprié de l'information et d'une démarche éthique visant à informer et conscientiser les utilisateurs des risques potentiels et des règles en vigueur.

5.04 Le Collège adhère aux principes de partage des meilleures pratiques en matière de sécurité de l'information, s'appuie sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et a recours à des barèmes de comparaison avec des organismes ou des établissements similaires.

5.05 Le Collège adopte une approche basée sur le risque acceptable qui permet de protéger l'information tout au long de son cycle de vie.

5.06 Le Collège vise le maintien d'un équilibre entre l'accès aux outils permettant la prestation de travail et la sécurité de l'information.

ARTICLE 6.00 – GESTION DES ACCÈS

La gestion des accès s'effectue conformément aux prescriptions de la Politique sur l'utilisation des technologies de l'information (PO-27). Elle doit être encadrée et contrôlée afin que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le but de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

ARTICLE 7.00 – GESTION DES RISQUES

La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Collège. L'investissement dans une procédure proactive est nécessaire pour que le Collège puisse prévoir des solutions pour minimiser sa vulnérabilité.

Par la présente Politique, le Collège s'engage à :

7.01 Créer et tenir à jour une catégorisation des actifs informationnels du Collège afin de connaître la nature et la valeur de l'information à protéger ;

7.02 Déterminer le niveau de risque acceptable par le Collège ;

7.03 Évaluer qualitativement et quantitativement les dommages potentiels qu'un incident pourrait causer ;

7.04 Identifier les vulnérabilités exploitables : probabilités d'accident, d'erreur ou de malveillance ;

7.05 Déterminer les moyens de mitigation à mettre en place pour minimiser les risques ;

7.06 Guider 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 Collège ;

7.07 Déclarer les risques à portée gouvernementale conformément à la Directive sur la sécurité de l'information gouvernementale.

ARTICLE 8.00 – GESTION DES INCIDENTS

Le Collège se doit d'assurer la continuité de ses services face aux incidents et aux incidents de sécurité de l'information à portée gouvernementale. À cet égard, il met en place les mesures nécessaires à l'atteinte des buts suivants :

8.01 Réduire la vulnérabilité du Collège face aux incidents en matière de sécurité de l'information ;

8.02 Gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations :

8.02.01 Corriger les vulnérabilités connues ;

8.02.02 Entreprendre les actions pour rétablir les services affectés par un incident, avant que celui-ci n'ait des répercussions sur les utilisateurs ;

8.02.03 Redonner l'accès complet ou partiel au service affecté, en réduisant les conséquences portant sur les opérations du Collège ;

8.03 Déclarer les incidents de sécurité de l'information à portée gouvernementale conformément à la Directive sur la sécurité de l'information gouvernementale ;

8.04 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 9.00 – RÔLES ET RESPONSABILITÉS

9.01 Utilisateurs

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

Chaque utilisateur s'engage à :

9.01.01 Respecter la présente Politique ;

9.01.02 Respecter les mesures de sécurité mises en place, sans les contourner, ni modifier leur configuration ou les désactiver ;

9.01.03 Informer la DTI de tout incident de sécurité de l'information (piratage ou intrusion d'un système informatique, vol d'identité, utilisation de virus informatique, etc.) dont il a connaissance.

L'employé utilisateur doit :

9.01.04 Participer à la catégorisation de l'information de son service ;

9.01.05 Signaler à son supérieur immédiat tout incident susceptible de constituer une contravention à la présente Politique ou de constituer une menace à la sécurité de l'information du Collège ;

9.01.06 Sauvegarder toute information institutionnelle conformément aux prescriptions de la Directive sur l'utilisation de l'infonuagique (D-24).

Le fournisseur externe qui, dans le cadre d'un mandat confié par le Collège, utilise ou accède aux actifs informationnels doit :

9.01.07 S'assurer que lui et ses employés respectent la présente Politique et signalent tout incident susceptible de constituer une contravention à la présente Politique ou de constituer une menace à la sécurité de l'information du Collège.

9.02 Gestionnaire – Supérieur immédiat

Le gestionnaire, responsable d'un service ou d'une unité administrative, doit :

9.02.01 Présenter la présente Politique à son personnel et aux tiers avec lesquels ils transigent dans le but qu'ils s'y conforment et afin que les exigences en matière de sécurité de l'information soient respectées dans tout processus et tout contrat sous sa responsabilité ;

9.02.02 Collaborer activement à la catégorisation de l'information de son service ou de son unité administrative, ainsi qu'à l'analyse de risques ;

9.02.03 Voir à la protection de l'information et des systèmes d'information sous sa responsabilité et veiller à ce que ceux-ci soient utilisés en conformité avec la présente Politique ;

9.02.04 Rapporter à la DTI toute menace ou tout incident menaçant la sécurité de l'information ;

9.02.05 Collaborer 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 ;

9.02.06 Rapporter à la DTI tout problème lié à l'application de la présente Politique ;

9.02.07 Gérer les accès aux différents systèmes ou logiciels des utilisateurs sous sa responsabilité et d'informer la DTI du retrait des accès le cas échéant ;

9.02.08 Faire signer une entente de confidentialité lorsque requis.

9.03 Direction des ressources matérielles (DRM)

La DRM participe, avec le directeur de la DTI, à l'identification et à la mise en place des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Collège.

Plus particulièrement, la DRM doit :

9.03.01 S'assurer de la mise au rebut sécuritaire des supports de l'information ;

9.03.02 Élaborer et mettre en œuvre des directives, des guides et des procédures propres à son domaine d'intervention ;

9.03.03 S'assurer que les salles informatiques, salle des serveurs et salles de télécommunication, sont uniquement accessibles par des employés de la DTI et du Service de la sécurité et de la prévention ;

9.04 Direction des technologies de l'information (DTI)

La DTI 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.

Plus particulièrement, la DTI doit :

9.04.01 Participer 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 ;

9.04.02 Appliquer des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, notamment l'interruption ou la révocation temporaire des services d'un système d'information ;

9.04.03 Mettre en place un plan de continuité des services en vue de rétablir les services essentiels à la communauté, selon un délai prévu.

9.05 L’analyste en sécurité de l’information

L’analyste en sécurité de l’information, sous la supervision du RSI, soumet ses recommandations en matière de sécurité de l'information et tout autre élément pouvant être nécessaire pour assurer la protection du Collège et être conforme à la réglementation.

Il doit :

9.05.01 Mettre en place les plans d’action et les bilans de sécurité de l’information, les activités de sensibilisation ou de formation, ainsi que toute proposition d’action en matière de sécurité de l’information ;

9.05.02 Il assure la coordination, la gestion et la supervision de comités ad hoc de mise en œuvre, d’implantation et de mesures opérationnelles.

9.06 Coordonnateur organisationnel de gestion des incidents (COGI)

Le COGI participe activement au réseau d’alerte gouvernemental et collabore étroitement avec le directeur des technologies de l’information et l’analyste en sécurité de l’information.

Il doit notamment :

9.06.01 Collaborer au processus sectoriel de gestion des incidents de sécurité de l’information et du processus gouvernemental de gestion des incidents ;

9.06.02 S'assurer que le registre des incidents soit tenu à jour, que les incidents soient documentés et que le Directeur des technologies de l’information soit tenu informé ;

9.06.03 Contribuer à l’analyse des risques de sécurité et à la mise en œuvre des solutions appropriées ;

9.06.04 Assurer la coordination de l’équipe de réponse aux incidents de sécurité de l’information des organismes publics qui lui sont rattachés et mettre en œuvre les stratégies de réaction appropriées ;

9.06.05 S'assurer que des guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunication soient élaborés et tenus à jour ;

9.06.06 Contribuer, conjointement avec le dirigeant principal de l’information et le CERT/AQ, à la définition et à la mise en œuvre du processus de gestion des incidents à portée gouvernementale ;

9.06.07 Coordonner l’élaboration du plan de continuité des services, veiller à sa mise en œuvre et en assurer la mise à jour ;

9.06.08 Assurer la planification et la coordination des tests initiaux et récurrents.

En tant que responsable de la vérification interne il doit également évaluer, examiner ou vérifier, notamment :

9.06.09 L’application, la validité et l’efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l’information élaborés et mis en œuvre ;

9.06.10 L’intégration de la sécurité de l’information dans les processus d’affaires.

9.07 Direction des technologies de l'information (DTI)

Dans le cadre de ses fonctions, le DTI est le RSI. Il s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins.

Celui-ci doit notamment :

9.07.01 Élaborer le programme de sécurité de l'information du Collège, le présenter et rendre compte de son implantation au comité de direction ;

9.07.02 Formuler des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information ;

9.07.03 Produire les bilans et les redditions de comptes du Collège en matière de sécurité de l'information et veiller à ce que la présente Politique soit mise à jour ;

9.07.04 Assurer la coordination et la cohérence des actions menées au sein du Collège en matière de sécurité de l'information en conseillant ou en formant les gestionnaires le cas échéant ;

9.07.05 S'assurer, en collaboration avec le Secrétariat général, que la Politique soit respectée par tout fournisseur externe qui a accès aux actifs informationnels, et ce, au moyen d'ententes contractuelles ;

9.07.06 Voir à la production, par le Collège, de la déclaration des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ) ;

9.07.07 Collaborer à l'élaboration du contenu d'un plan de communication, d'un programme de sensibilisation et de formation en matière de sécurité de l'information et veiller au déploiement de ceux-ci ;

9.07.08 Procéder aux enquêtes conformément aux prescriptions de la Politique sur l'utilisation des technologies de l'information (PO-27) et en faire rapport au Comité de direction du Collège ;

9.07.09 S'assurer 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 ;

9.07.10 Tenir à jour le registre des dérogations et le registre des cas de contravention à la présente Politique.

9.08 Secrétariat général

Le secrétariat général est responsable de l'accès à l'information et de la protection des renseignements personnels et veille au respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1).

À ce titre, il doit :

9.08.01 Communiquer au directeur des technologies de l'information les problématiques et les préoccupations de sécurité en matière de protection des renseignements personnels ou à caractère sensible ;

9.08.02 Contribuer à assurer la cohérence et l'harmonisation des interventions entre la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information.

En tant que responsable de la gestion documentaire il doit également :

9.08.03 Superviser la catégorisation de l'information ;

9.08.04 Collaborer à la conception des systèmes informatiques, administratifs ou autres et s'assurer qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires à une saine gestion des connaissances et du patrimoine informationnel, à la préservation des preuves et au respect des lois ;

9.08.05 Collaborer étroitement avec les gestionnaires et l'analyste en sécurité de l'information, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

En tant que responsable de l'éthique en matière de gouvernance, le Secrétariat général veille à l'intégration de l'éthique dans les processus de gestion de la sécurité de l'information.

ARTICLE 10.00 – LES COMITÉS

10.01 Comité de gouvernance numérique (CGN)

Les membres ont pour mandat d'informer le comité des risques et enjeux de sécurité liés à leur domaine d'action, afin qu'ils soient discutés.

Le CGN, en matière de sécurité de l'information, doit notamment :

10.01.01 Examiner et formuler des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action, ainsi que toute proposition d'action ou état d'avancement de projets en sécurité de l'information ;

10.01.02 Analyser et formuler des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information du Collège.

10.02 Comité de continuité des services

Le comité de continuité des services est principalement composé du RSI, du COGI et de l'analyste en sécurité de l'information.

Il a pour rôle, notamment :

10.02.01 De procéder à l'évaluation des dommages ;

10.02.02 D'assurer la mise en œuvre du plan de mobilisation ;

10.02.03 D'assurer la coordination avec les intervenants externes.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans ses prises de décision. Il est présidé par le responsable de la continuité des services ou son représentant.

ARTICLE 11.00 – SANCTIONS

11.01 Quiconque contrevient à une disposition de la présente Politique est passible de sanctions proportionnelles à la gravité de son acte :

11.01.01 La suspension de ses droits d'accès aux actifs informationnels du Collège ;

11.01.02 L'expulsion immédiate des lieux ;

11.01.03 La réprimande écrite versée au dossier ;

11.01.04 La réparation des dommages causés ;

11.01.05 La suspension pour une période d'une durée déterminée ;

11.01.06 Le renvoi ou le congédiement.

11.02 Dans le cas de membres du personnel, l'application des sanctions prévues au présent article doit se faire conformément aux conventions collectives de travail auxquelles le Collège est partie ou dans les politiques de gestion de personnel.

11.03 Les autorités responsables de l'application des sanctions prévues à la présente Politique peuvent, s'ils le jugent pertinent, s'adjoindre des experts dans des domaines spécifiques, notamment en informatique, afin de faire la lumière sur les faits et circonstances entourant les contraventions à la présente Politique.

ARTICLE 12.00 – RESPONSABLE DE LA POLITIQUE

La direction des technologies de l'information est responsable de l'application de la Politique.

ARTICLE 13.00 – ENTRÉE EN VIGUEUR

a) La présente Politique entre en vigueur à la date de son adoption par le Conseil d'administration, soit le 28 novembre 2018.

b) La révision et la mise à jour de la Politique sont prévues au besoin ou au plus tard aux cinq (5) ans.