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

Amendée le 14 juin 2023

TABLE DES MATIERES

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

PRÉAMBULE

Le Collège Ahuntsic a notamment pour mission d'offrir l'enseignement général et professionnel de niveau collégial. Il accompagne et soutient les personnes étudiantes dans leur projet d'études. Il contribue, en outre, à l'élaboration et à la réalisation de projets d'innovation technologique, à l'implantation de technologies nouvelles et à leur diffusion, ainsi qu'au développement de la région, le tout grâce à des activités de formation de la main-d'œuvre, de recherche appliquée et d'aide technique à l'entreprise. Il effectue des études ou de la recherche et soutient les membres de son personnel qui participent à des programmes subventionnés de recherche. Il permet l'utilisation de ses installations et équipements à des fins culturelles, sociales, sportives ou scientifiques. Finalement, il participe à l'élaboration et à la réalisation de programmes de coopération avec l'extérieur dans le domaine de l'enseignement collégial. Dans le cadre de cette mission, le Collège doit recueillir, produire et détenir des informations.

Cette Politique contribue à l'accomplissement de la mission du Collège et vise à préserver sa réputation, à respecter les lois et à réduire les risques d'incidents liés au traitement des données en protégeant l'information qu'il a créée ou reçue et dont il est le gardien. Cette information, multiple et diversifiée, est constituée notamment des renseignements personnels des personnes étudiantes et des membres du personnel, de l'information professionnelle sujette à des droits de propriétés intellectuelles et, finalement, de l'information stratégique ou opérationnelle pour l'administration du Collège. Le Collège est interconnecté 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*, de la Directive sur la sécurité de l'information gouvernementale et de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* oblige 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 personnes qui doivent intervenir 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.

Enfin, les actifs informationnels que détient le Collège étant essentiels à ses activités courantes, la présente Politique établit les règles visant à préserver adéquatement la confidentialité, à garantir l'intégrité et à assurer la disponibilité de l'information, selon les pratiques exemplaires en matière de sécurité de l'information, tant sur le plan national qu'international.

ARTICLE 1.00 – ABRÉVIATIONS ET DÉFINITIONS

1.01 Abréviations

a) **CERT/AQ** : Computer Emergency Response Team/Administration québécoise ;
b) **COCD** : Centre opérationnel de cyberdéfense ;
c) **DRM** : Direction des ressources matérielles ;
d) **DTI** : Direction des technologies de l'information ;
e) **MCN :** Ministère de la cybersécurité et du numérique ;

f) MERN : Ministère de l'Énergie et des Ressources naturelles ;

1.02 Définitions

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

a) **« ACTIF INFORMATIONNEL » :** Information numérique, document numérique ou analogique, système d'information, documentation, matériel informatique, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitués par le Collège pour mener à bien sa mission, qu'ils soient détenus ou exploités par le Collège, par des prestataires de services ou par des tiers.

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 responsable de répondre aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale.

d) **« CONFIDENTIALITÉ »** : Propriété des informations ou des 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) « ÉVITEMENT D'UN RISQUE » : Décision consciente de ne pas entreprendre une activité particulière ou de trouver un moyen que le risque ne se réalise pas.

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

h) **« INCIDENT »** : Évènement 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.

i) **« INCIDENT DE CONFIDENTIALITÉ »** : Accès non autorisé par la loi à un renseignement personnel, son utilisation ou sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

j) **« 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.

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

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

m) **« 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.

n) **« 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.

o) « **NON-RÉPUDIATION** » : Impossibilité pour une partie de nier avoir participé en totalité ou en partie à un échange, du fait de l'existence de contrôles d'authentification, d'accusés de réception et de pistes d'audit efficaces.

p) **« PILOTE DE SYSTEME »** : Utilisateur ou utilisatrice du système, qui se charge des configurations avancées dans le système et qui a l'autorisation d'exécuter des fonctions liées à la sécurité. Les pilotes de système sont aussi responsables de faire des essais d'utilisation avant les mises en production du système.

q) **« PROPRIETAIRE DE SYSTEME » :** Dans l'organisation, personne responsable de l'acquisition, du développement, de l'intégration, de la modification, de l'exploitation, de la maintenance et de l'élimination d'un système.

r) **« 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.

s) **« PLAN DE RELÈVE »** : 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 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.

t) **« 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.

u) **« 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~~, ainsi que le suivi.

v) **« 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 cartes de paiement.

w) **« RISQUE MAXIMAL ACCEPTABLE » :** Capacité objective de l'organisation à poursuivre ses activités malgré la réalisation d'un risque informatique. Seuil de risque au-delà duquel les actifs informationnels sont menacés de façon intolérable.

x) **« 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.

y) **« 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.

z) **« 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.

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

bb) **« 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.

cc) « TRANSFERT D'UN RISQUE » : Action de faire passer le risque à un tiers en souscrivant une assurance ou en transférant ce risque par contrat à une entité autre qu'une compagnie d'assurance par exemple.

dd) **« UTILISATEUR OU UTILISATRICE » :** Toute personne physique ou morale utilisant ou ayant accès aux actifs informationnels du Collège. Entrent notamment dans cette catégorie le personnel enseignant, le personnel professionnel, le personnel de soutien, le personnel cadre, la population étudiante, les organisations syndicales ou associatives qui les représentent, les locataires de la résidence étudiante, les personnes retraitées du Collège, ainsi que les prestataires de services 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 la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, le Collège doit veiller à assurer :

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

b) L'intégrité de l'information afin 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 avec les lois et les directives gouvernementales ainsi qu'aux autres besoins du Collège en matière de réduction du risque associé à la protection de l'information.

2.04 Atteindre une maturité adéquate et une compréhension commune de la sécurité de l'information et de l'engagement constant de tous les utilisateurs et utilisatrices, plus précisément :

a) Assurer que l'utilisatrice ou l'utilisateur soit conscient et tenu informé de sa responsabilité en matière de sécurité de l'information ;

b) Développer une culture organisationnelle qui prenne en compte la sécurité de l'information dans les activités quotidiennes.

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 ;

l) Les exigences du ministère de la Cybersécurité et du numérique et du Centre opérationnel de cyberdéfense

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

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

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

c) Directive sur l'utilisation de l'infonuagique (D-24) ;

d) Directive de la gestion des identités et des accès (D-26) ;

e) Règlement relatif à la sécurité et à la protection des personnes et des biens (R-14).

ARTICLE 4.00 – CHAMP D'APPLICATION

4.01 La présente Politique s'adresse à tous les utilisateurs et utilisatrices, c'est-à-dire à toute personne physique ou morale ayant accès à l'information et aux actifs informationnels du Collège indépendamment de l'endroit où ceux-ci sont utilisés ;

4.02 La présente Politique s'applique à tous les actifs informationnels du Collège, durant tout leur cycle de vie, qu'ils soient conservés par le Collège ou par un tiers ;

4.03 La présente Politique s'applique à toute activité, incluant, mais sans s'y limiter, la création, la

collecte, l'utilisation, le traitement, la communication, la conservation ou la destruction d'une information ou d'un actif informationnel appartenant au Collège, qu'elle soit conduite dans ses locaux, dans un autre lieu ou à distance ;

ARTICLE 5.00 – PRINCIPES DIRECTEURS

5.01 Le Collège assure la sécurité de l'information en la protégeant des risques d'accident, des erreurs et des actes malveillants auxquels elle est exposée. Il assure également la protection des renseignements personnels de toute divulgation, de tout accès ou de toute utilisation non autorisée.

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

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

5.04 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 des actifs informationnels et d'une démarche éthique visant à informer et conscientiser tout utilisateur ou utilisatrice sur les risques et les règles en vigueur.

5.05 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.

5.06 Le Collège adopte une approche basée sur le risque maximal acceptable qui permet de protéger l'information et d'assurer sa fiabilité tout au long de son cycle de vie.

5.07 Le Collège s'engage, sur une base régulière, à sensibiliser et à former les utilisateurs et utilisatrices à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et à leurs obligations en la matière.

5.08 Le Collège exerce, en conformité avec la législation et la règlementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels.

ARTICLE 6.00 - CADRE DE GESTION

La présente politique fait partie d'un ensemble de mesures visant la protection des actifs informationnels. Elle sera complétée par des directives touchant des domaines d'application particuliers de sécurité de l'information, ainsi que les dispositions et mesures de sécurité de l'information à respecter. Des directives seront adoptées et mises en place, entre autres et de façon non restrictive, sur la gestion des accès et de l'échange sécuritaire de l'information, sur la sécurité physique des locaux et des équipements, sur la gestion de la reprise et de la continuité des affaires, sur la gestion des contractants et des contrats, et sur l'utilisation et la protection des supports amovibles (mémoires Flash, disques durs, etc.)[1].

ARTICLE 7.00 – GESTION DES ACCÈS

[1] Ministère de l'Énergie et des Ressources naturelles, ministère des Forêts, de la Faune et des Parcs. (2021). *Politique de sécurité de l'information*. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/energie-ressources-naturelles/publications-adm/politique/PO-securite-information-MERN.pdfb

La gestion des accès s'effectue conformément aux prescriptions de la Directive de la gestion des identités et des accès (D-26). 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 8.00 – GESTION DES RISQUES

La mise en œuvre d'une gouvernance intégrée de la sécurité de l'information nécessite la mise en place d'un processus de gestion des risques basé sur l'amélioration continue permettant l'identification, l'analyse et le traitement des risques de sécurité et des risques à tous les niveaux hiérarchiques du Collège. L'investissement dans une procédure proactive est nécessaire afin que le Collège puisse prévoir des solutions pour minimiser sa vulnérabilité.

Sur une base récurrente, une analyse de risques est effectuée afin d'identifier les risques pouvant affecter la réalisation de la mission du Collège. Les actifs informationnels sont catégorisés par la personne détentrice selon le plan de catégorisation de l'information en vigueur au Collège, et ce, dès l'étape de la conception. Ils sont protégés selon le besoin en matière de disponibilité, d'intégrité et de confidentialité, de façon à considérer les mesures applicables en sécurité de l'information. Le choix des mesures de protection s'appuie sur une analyse des risques auxquels l'information peut être exposée.

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

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

8.02 De recourir à l'évitement ou au transfert de risques ;

8.03 Mitiger les risques lorsqu'ils sont inévitables, et n'accepter les risques qu'en cas de force majeure ;

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

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

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

8.07 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 ;

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

ARTICLE 9.00 – GESTION DES INCIDENTS

Le Collège doit 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 :

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

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

9.02.01 Corriger les vulnérabilités connues ;

9.02.02 Entreprendre les actions pour rétablir les services affectés par un incident, avant que celui-ci n'entraine des répercussions sur les utilisateurs et utilisatrices ;

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

9.03 Gérer les incidents de confidentialité conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ;

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

9.05 Exercer ses pouvoirs et ses prérogatives à l'égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

9.06 Suivre le processus de gestion des menaces, des vulnérabilités et des incidents (GMVI), du gouvernement.

ARTICLE 10.00 – RÔLES ET RESPONSABILITÉS

10.1 Utilisateurs et utilisatrices

Toute personne qui accède à une information est responsable de l'utilisation qu'elle en fait et doit procéder de manière à protéger cette information, tant au collège qu'à l'extérieur de celui-ci, notamment en situation de télétravail, d'enseignement à distance ou d'apprentissage à distance.

Chaque utilisateur ou utilisatrice s'engage à :

10.1.1 Prendre connaissance de la présente Politique et la respecter ;

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

10.1.3 Se conformer aux exigences légales portant sur l'utilisation de produits (logiciels, progiciels, applications) ou de documents à l'égard desquels des droits de propriété intellectuelle pourraient exister ;

10.1.4 Informer immédiatement 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 ou elle a connaissance.

10.1.5 Au moment de son départ définitif du Collège, remettre les différentes cartes d'identité et d'accès, les clés, les actifs informationnels, quel qu'en soit le support, ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de ses fonctions. Ces actifs informationnels doivent être vidés du contenu personnel. Exceptionnellement, la personne qui utilise des actifs informationnels à des fins personnelles peut faire une demande à la DTI pour lui rendre disponibles certains renseignements de nature personnelle. Si ceux-ci sont encore disponibles, leurs modalités de transmission seront alors convenues avec la DTI.

10.1.6 Utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés ou aux fins autorisées dans les politiques du Collège ;

10.1.7 Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout

équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver ;

Le personnel utilisateur doit :

10.1.8 Participer aux activités de formation et de sensibilisation à la cybersécurité ;

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

10.1.10 Signaler à son supérieur immédiat ou sa supérieure immédiate tout incident susceptible de constituer une contravention à la présente Politique ou de constituer une menace à la sécurité de l'information du Collège, dès qu'il en a connaissance ;

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

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

10.1.12 S'assurer que lui ou elle et les personnes à son emploi 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, et ce, dès qu'il ou elle en a connaissance.

10.2 Gestionnaire – Supérieur immédiat ou supérieure immédiate

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

10.2.1 Fournir la présente Politique à son personnel et aux tiers prestataires externes avec lesquels il ou elle collabore dans le but que tous 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 ;

10.2.2 Consulter la DTI pour tout projet informatique afin qu'une analyse de risques soit réalisée ;

10.2.3 Consulter le comité permanent sur l'accès aux documents et la protection des renseignements personnels pour tout projet d'acquisition, de développement ou de refonte de système d'information qui implique la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels afin de réaliser une évaluation des facteurs relatifs à la vie privée ;

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

10.2.5 Voir à la protection des actifs informationnels sous sa responsabilité et veiller à ce que ceux-ci soient utilisés en conformité avec la présente Politique ;

10.2.6 Rapporter à la DTI toute menace ou tout incident menaçant la sécurité de l'information, et ce, dès qu'il ou elle en a connaissance ;

10.2.7 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 ;

10.2.8 Rapporter à la DTI tout problème lié à l'application de la présente Politique, et ce, dès qu'il ou elle en a connaissance ;

10.2.9 Gérer et ajuster les droits aux cartes d'accès, aux clés, aux actifs informationnels quel

qu'en soit le support, des utilisateurs et utilisatrices sous sa responsabilité, et informer le pilote et le propriétaire de l'actif informationnel du retrait des accès le cas échéant conformément aux prescriptions de la Directive de la gestion des accès et des identités (D-26) ;

10.2.10 Faire signer une entente de confidentialité lorsque requis ;

10.2.11 S'assurer, lorsque lui ou elle, ou son personnel procède à la destruction de documents contenant des renseignements personnels, de prendre les mesures de protection nécessaires visant à assurer la confidentialité de ceux-ci. La méthode de destruction utilisée doit être déterminée en fonction de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

10.3 Direction des ressources matérielles (DRM)

La DRM participe, avec le directeur ou la directrice 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 :

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

10.3.2 S'assurer que les salles des serveurs et salles de télécommunication sont uniquement accessibles par des membres du personnel de la DTI, de la maintenance et du Service de la sécurité et de la prévention qui ont un réel besoin d'y accéder pour exploiter, sécuriser ou entretenir l'espace ;

10.4 Direction des ressources humaines

La direction des ressources humaines remet à toute personne nouvellement embauchée par le Collège un document d'accueil indiquant les liens vers les règlements, les politiques et les directives qui ont un lien avec la protection de l'information, notamment la *Politique sur l'utilisation des technologies de l'information* (PO-27), la présente Politique et les directives qui en découlent.

10.5 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 :

10.5.1 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 ;

10.5.2 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 ;

10.5.3 Mettre en place un plan de continuité des services en vue de rétablir les services essentiels à la communauté ;

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

10.5.5 Former une équipe de sécurité de l'information ;

10.5.6 Procéder à l'évaluation des dommages en cas de cyberattaque ;

10.5.7 D'assurer la mise en œuvre du plan des mesures d'urgence ;

10.5.8 D'assurer la mise à jour du plan des mesures d'urgence ;

10.5.9 Assurer la mise en œuvre du plan de relève ;

10.5.10 Assurer la coordination avec les intervenants externes.

10.6 L'équipe de sécurité de l'information de la DTI

L'équipe de sécurité de l'information, sous la supervision du directeur ou de la directrice des technologies de l'information, 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 règlementation.

Elle doit :

10.6.1 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 ;

10.6.2 Assurer la coordination, la gestion et la supervision de comités ad hoc de mise en œuvre, d'implantation et de mesures opérationnelles.

10.7 Directeur adjoint ou directrice adjointe à l'infrastructure

Le directeur adjoint ou la directrice adjointe à l'infrastructure effectue la coordination des mesures de sécurité de l'information et de la gestion des incidents. Cette personne collabore étroitement avec le directeur ou la directrice des technologies de l'information et l'analyste en sécurité de l'information.

Son rôle est notamment de :

10.7.1 Collaborer au processus sectoriel de gestion des incidents de sécurité de l'information et du processus gouvernemental de gestion des incidents ;

10.7.2 S'assurer que le registre des incidents soit tenu à jour, que les incidents soient documentés et que le Directeur ou la Directrice des technologies de l'information reçoive l'information ;

10.7.3 Informer le secrétariat général de tout incident touchant les renseignements personnels afin qu'il soit consigné au registre tenu à cette fin ;

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

10.7.5 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 ;

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

10.7.7 Contribuer, conjointement avec la personne dirigeante responsable 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 ;

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

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

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

10.7.10 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 ;

10.7.11 L'intégration de la sécurité de l'information dans les processus d'affaires.

10.8 Directeur ou directrice de la DTI

Dans le cadre de ses fonctions, le directeur ou la directrice de la DTI est la personne responsable organisationnelle de la sécurité de l'information. Il ou elle s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins.

Cette personne doit notamment :

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

10.8.2 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 ;

10.8.3 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 ;

10.8.4 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 ;

10.8.5 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 ;

10.8.6 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) ;

10.8.7 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 ;

10.8.8 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 ;

10.8.9 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 ;

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

10.9 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 :

10.9.1 Communiquer à la direction des technologies de l'information les problématiques et les préoccupations de sécurité en matière de protection des renseignements personnels ou à caractère sensible ;

10.9.2 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.

10.9.3 Tenir et maintenir à jour un registre des incidents touchant les renseignements personnels ;

10.9.4 S'assurer que le comité permanent sur la protection des renseignements personnels soit consulté pour tout projet d'acquisition, de développement ou de refonte d'un système d'information qui implique la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels afin de réaliser une évaluation des facteurs relatifs à la vie privée ;

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

10.9.5 Superviser la catégorisation de l'information ;

10.9.6 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 ;

10.9.7 Collaborer étroitement avec les gestionnaires et l'équipe de 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 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 en conformité avec le Règlement relatif à la sécurité et à la protection des personnes et des biens (R-14).

11.02 En plus des sanctions incluses au Règlement relatif à la sécurité et à la protection des personnes et des biens (R-14), une plainte peut être déposée auprès des autorités policières.

11.03 Le Collège se réserve le droit d'entamer des poursuites en dommages et intérêts.

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 tous les cinq (5) ans.