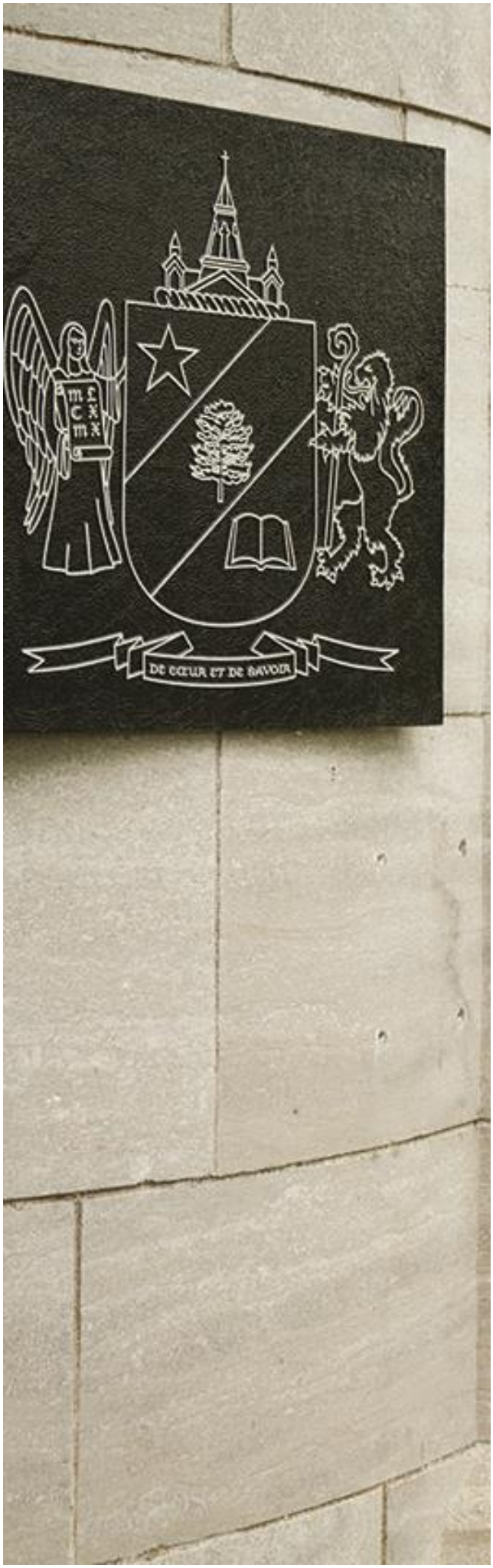

cegep de Saint-Jérôme
SAINT-JÉRÔME
MONT-TREMBLANT
MONT-LAURIER

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Adoptée par le conseil d'administration le 20 octobre 2020

DIRECTION DES ÉTUDES
CÉGEP DE SAINT-JÉRÔME

Mention de source :

La présente *Politique sur la sécurité de l'information* s'inspire du gabarit préparé par la Fédération des cégeps ainsi que des politiques adoptées récemment par d'autres collèges, dont celles du Cégep Édouard-Montpetit et du Collège Ahuntsic.

TABLE DES MATIÈRES

PRÉAMBULE

La *Politique sur la sécurité de l'information* (ci-après la Politique) vise à doter le Cégep de Saint-Jérôme (ci-après le Collège) de balises lui permettant de protéger l'information créée, reçue ou conservée dans le cadre de ses activités. Cette information est multiple et diversifiée et elle doit faire l'objet d'une utilisation appropriée et d'une protection adéquate. Elle consiste en des renseignements personnels d'étudiantes et d'étudiants ainsi que de membres du personnel, en de l'information professionnelle qui pourrait selon le cas être soumise à des droits de propriété intellectuelle (personnel enseignant et résultats de recherche) et, finalement, en de l'information stratégique ou opérationnelle pour l'administration du Collège.

L'interconnectivité des systèmes et de l'information place les collèges devant l'obligation d'assurer une gestion des accès et de l'information, que ces derniers soient numériques ou physiques. Dans ce contexte, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre. G-1.03) et la *Directive sur la sécurité de l'information gouvernementale* (Recueil des politiques de gestion du Conseil du trésor) font état des obligations auxquelles doivent se conformer tous les organismes publics quant à l'adoption, à la mise en œuvre et au suivi de l'application d'une politique de sécurité de l'information. Les principales modalités sont définies dans la directive gouvernementale et elles font référence notamment à des processus et des normes de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion des accès et la gestion des incidents.

En conséquence, le Collège met en place la présente Politique qui oriente et détermine le partage des responsabilités entre les différents intervenants ainsi que l'utilisation appropriée et sécuritaire de l'information et des technologies de l'information.

OBJECTIFS

La présente Politique a pour principal objectif de définir les balises et d'affirmer l'engagement du Collège à s'acquitter pleinement de ses obligations légales à l'égard de la sécurité de l'information, quels que soient son support ou les moyens technologiques ou de communication utilisés. Plus précisément, le Collège doit veiller à assurer :

- la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par les personnes autorisées ;

- l'intégrité de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues, en conformité avec le calendrier de conservation du Collège ;

- la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées et aux fins prévues.

Pour encadrer la mise en œuvre de cette Politique, le Collège se dote d'un cadre de gestion de la sécurité de l'information, qui comprendra des procédures, directives et guide afin de préciser les obligations qui en découlent. Le cadre de gestion viendra renforcer les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi que des besoins du Collège en matière de réduction du risque associé à la protection de l'information.

CADRE RÈGLEMENTAIRE

La Politique sur la sécurité de l'information s'inscrit notamment dans un contexte régi par :

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

- le *Code civil du Québec* (LQ, chapitre 64, 1991) ;

- 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, chapitre C-46, 1985) ;

- 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* (Conseil du trésor, vol. 11, 2.2.2) ;

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

- les autres règlements, politiques, procédures, guides et conventions collectives en vigueur au Collège.

DÉFINITIONS

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

Actif informationnel : La *Loi concernant le cadre juridique des technologies de l'information* (LRQ., chapitre C-1.1) définit l'actif informationnel sans égard au support comme étant : « [Un ensemble] constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles. » Cette même loi assimile au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci[1].

Continuité des services : Capacité du Collège d'assurer, en cas de sinistre, la poursuite de ses activités, selon un niveau de service prédéfini par catégorie d'actifs informationnels[2].

Cycle de vie de l'information : L'ensemble des étapes que franchit l'information, de sa conception en passant par son enregistrement, son transfert, sa consultation, son traitement et

[1] CONSEIL DU TRÉSOR. *Guide d'élaboration d'une politique de sécurité de l'information*.
[2] Ibid.

sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation du Collège.

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

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, par exemple une interruption des services ou une réduction de leur qualité.

Information : Renseignement consigné sur tout support pour être conservé, traité ou communiqué.

Intégrité : Propriété d'une information de ne subir aucune altération ni destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude de l'information.

Mesure de sécurité de l'information : Moyen concret assurant, partiellement ou totalement, la protection d'information du Collège contre un ou plusieurs risques et dont la mise en œuvre vise à amoindrir la probabilité de survenue de ces risques ou à réduire les pertes qui en résultent[3].

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.

Registre d'autorité : Répertoire, recueil ou fichier dans lesquels sont notamment consignées les désignations effectuées et les délégations consenties pour les besoins de la gestion de la sécurité de l'information ainsi que les responsabilités afférentes.

Registre d'incident : recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, son impact, les mesures prises pour la reprise des activités et le suivi.

Renseignement personnel : tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* n'est pas considéré comme un renseignement personnel dans le cadre de cette Politique[4].

[3] Ibid.
[4] QUÉBEC. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, art. 54 .

Ressources informationnelles : Les actifs informationnels, ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs[5].

Risque lié à la 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 du service 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 de services, sur la vie, la santé ou le bien-être des personnes, sur la protection des renseignements personnels, le respect de leur vie privée ou sur l'image du Collège.

Risque à portée gouvernementale : Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale, 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[6].

Système d'information : Ensemble organisé de moyens permettant de recueillir, d'emmagasiner, de traiter, de communiquer, de protéger ou d'éliminer l'information afin de répondre à un besoin précis, y compris les applications, logiciels, progiciels, technologies de l'information ainsi que les procédés utilisés pour accomplir ces fonctions.

Technologies de l'information : Regroupent principalement les techniques de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie) qui permettent aux personnes utilisatrices d'accéder aux sources d'information ou de communiquer, de stocker, de manipuler, de produire et de transmettre de l'information.

Personne utilisatrice : Toute personne physique ou morale autorisée à utiliser les actifs informationnels et les technologies de l'information du Collège, dans ses locaux ou à distance. Sont considérées comme des personnes utilisatrices les membres du personnel enseignant, du personnel professionnel, du personnel de soutien, du personnel d'encadrement, de la communauté étudiante ainsi que les tiers autorisés.

[5] CONSEIL DU TRÉSOR. *Guide d'élaboration d'une politique de sécurité de l'information*.
[6] CONSEIL DU TRÉSOR. *Cadre gouvernemental de gestion en matière de Sécurité de l'information*.

CHAMP D'APPLICATION

La présente Politique s'applique à toutes les personnes utilisatrices du Collège, sans exception.

Cette politique s'applique également aux actifs informationnels qui appartiennent :

- au Collège et qui sont exploités par celui-ci ;
- au Collège et qui sont exploités par un fournisseur de services ou par un tiers ;
- à un fournisseur de services ou à un tiers et qui sont exploités par lui au bénéfice du Collège ;
- aux personnes utilisatrices et qui sont utilisés par le Collège ;
- au Collège et qui se retrouvent sur un équipement personnel des personnes utilisatrices.

Les activités visées par cette Politique sont la collecte, la consultation, la production, la transmission, la conservation et la destruction de l'information et des actifs informationnels, peu importe leur support, leur emplacement et le moyen de communication.

PRINCIPES DIRECTEURS

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

a) répertorier l'information à protéger et ses caractéristiques de sécurité et désigner les personnes qui en sont responsables ;

b) adhérer à une approche basée sur le risque acceptable au moyen de la mise en place d'un cadre de gestion permettant d'atténuer le risque, par une combinaison de mesures raisonnables mises en place pour garantir la sécurité de l'information, à un coût proportionnel à la sensibilité de l'information et aux effets potentiels ;

c) protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle ;

d) reconnaître que l'environnement technologique est en constante évolution et interconnecté avec le monde par la mise en place d'une gestion de la sécurité de l'information agile ;

e) reconnaître l'importance d'évaluer périodiquement les risques, de mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, de définir des mesures d'éradication des menaces ou de rétablissement des activités compromises ;

f) protéger l'information tout au long de son cycle de vie, et ce, peu importe son support ;

g) adhérer aux principes de communication des meilleures pratiques et de l'information opérationnelle en matière de sécurité de l'information au réseau de l'éducation et aux organismes publics ;

h) adhérer à une démarche éthique visant à assurer la régularisation des conduites et la responsabilisation individuelle (chaque personne qui a accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci) ;

i) permettre à chaque personne utilisatrice d'avoir accès uniquement aux renseignements qui sont nécessaires à l'exercice de ses fonctions ;

j) au minimum d'information requis pour accomplir ses tâches normales ;

k) communiquer de façon transparente au sujet des menaces pouvant affecter les actifs informationnels afin que chacun puisse comprendre l'importance d'appliquer la sécurité selon les exigences et être informé de façon à reconnaître les incidents de sécurité et à agir en conséquence ;

l) mettre en place un plan de continuité des activités en vue de rétablir les services aux personnes utilisatrices, selon un temps prévu par le responsable de l'actif informationnel.

CADRE DE GESTION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents acteurs du Collège, par la mise en place d'un cadre de gestion de la sécurité permettant notamment une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être remises en question de manière périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces et des risques.

La Politique sur la sécurité de l'information du Collège sera accompagnée d'un Guide de sensibilisation à la sécurité de l'information, de procédures et de directives de gestion, notamment celles relatives aux accès, aux risques et aux incidents.

Sensibilisation à la sécurité de l'information

La sécurité de l'information repose notamment sur la régularisation des conduites et la responsabilisation individuelle. À cet égard, les personnes utilisatrices doivent être sensibilisées :

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

À ces fins, un programme comportant des activités de sensibilisation et de formation est offert périodiquement aux personnes utilisatrices.

Gestion des accès

La gestion des accès doit être encadrée et contrôlée pour s'assurer que l'accès à l'information ainsi que sa divulgation et son utilisation sont strictement réservés aux personnes utilisatrices. Ces mesures sont prises dans le dessein de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

L’efficacité des mesures de sécurité de l’information repose sur l’attribution de responsabilités et la responsabilisation des personnes, à tous les échelons de personnel du Collège.

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 Collège.

La gestion des risques liée à la sécurité de l’information s’inscrit dans le processus global de gestion des risques du Collège. 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 notamment en fonction :

- de la nature de l’information et de son importance ;
- des probabilités d’accident, d’erreur ou de malveillance auxquelles elle est exposée ;
- des conséquences de la matérialisation de ces risques ;
- du niveau de risque acceptable par le Collège.

Gestion des incidents

Le Collège déploie des mesures de sécurité de l’information de manière à assurer la continuité de ses services à la suite des incidents et des incidents à portée gouvernementale. À cet égard, il met en place les mesures nécessaires à l’atteinte des buts suivants :

- réduire la vulnérabilité du Collège à l’égard des incidents en matière de sécurité de l’information ;
- gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou opérations :

- corriger les vulnérabilités connues ;

- appliquer les mesures de rétablissement des services affectés par un incident, avant que celui-ci n'ait des répercussions sur les personnes utilisatrices ;

- redonner l'accès complet ou partiel au service affecté, en réduisant les conséquences sur les opérations du Collège.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés par la coordination sectorielle de la gestion des incidents (CSGI) du Collège, conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Dans le cadre de la gestion des incidents, le Collège 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.

COMITÉ CHARGÉ DE LA SÉCURITÉ DE L'INFORMATION

Mandat

Le comité chargé de la sécurité de l'information est un comité ayant pour mandat de :

- conseiller le responsable de la sécurité de l'information (RSI), examiner et formuler des recommandations quant aux orientations, aux politiques, aux directives, aux cadres de gestion, aux mesures prioritaires, aux éléments de reddition de comptes ainsi qu'à tout événement ayant mis ou qui aurait pu mettre en péril la sécurité de l'information ;

- analyser et formuler des recommandations concernant le processus de gestion des risques et des incidents de sécurité de l'information à portée locale ou gouvernementale pour en assurer la cohérence ;

- soutenir le RSI dans de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'information ;

- coopérer à la mise en œuvre d'un programme institutionnel de formation et de sensibilisation en matière de sécurité de l'information ;

- assurer une veille quant à l'efficacité des moyens mis en place.

Afin de faciliter le fonctionnement du comité, des sous-comités pourront être formés afin de répondre à des activités ou besoins précis, notamment en matière de gouvernance numérique ou de continuité des services.

Composition

Le comité chargé de la sécurité de l'information est composé des intervenants suivants :

- Direction générale

- responsable de la sécurité de l'information (RSI)

- coordination du Service des affaires corporatives

- coordination sectorielle de la gestion des incidents (CSGI)

- coordination au maintien des actifs de la Direction des ressources matérielles

- responsable de la vérification interne à la Direction des finances et de l'approvisionnement

- membres du personnel d'encadrement responsables d'actifs informationnels désignés par le Collège provenant de chacune des directions, y compris un représentant des centres d'études collégiales et un représentant des centres collégiaux de transfert de technologie.

RÔLES ET RESPONSABILITÉS

La présente Politique attribue la gestion de la sécurité de l'information du Collège à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

Conseil d’administration

Le conseil d’administration adopte la Politique sur la sécurité de l’information ainsi que toute modification à celle-ci. Il nomme le responsable de la sécurité de l’information (RSI) et est informé annuellement des mesures prises par le Collège en matière de sécurité de l’information en qualité de dirigeant de l’organisme.

Direction générale

La Direction générale veille à l’application de la politique. Elle :

- préside le comité de sécurité de l’information ;
- encadre le responsable de la sécurité de l’information (RSI) dans la réalisation de son mandat ;
- délègue certaines responsabilités à la coordination du Service des affaires corporatives pour la gestion de l’information ;
- présente un rapport de l’application de la présente Politique au conseil d’administration ;
- autorise, de façon exceptionnelle, une dérogation à une disposition de la présente politique, d’une directive ou d’une procédure ayant une incidence directe ou indirecte sur la sécurité de l’information et qui serait incompatible avec une activité ou un projet qui se lie directement à la mission du Collège, sur recommandation du RSI ;
- autorise une enquête lorsqu’il y a ou il pourrait y avoir transgression sérieuse de la politique.

Comité de direction

Lorsque cela est requis, le comité de direction adopte les directives, guides et procédures qui viennent préciser ou soutenir l’application de la politique ou ses cadres de gestion. Il met en place les mesures nécessaires à l’application de la Politique et au respect des obligations légales du Collège en matière de sécurité de l’information.

Responsable de la sécurité de l’information (RSI)

Le conseil d’administration délègue à un cadre la fonction de responsable de la sécurité de l’information (RSI) et nomme ce dernier. Le RSI est le principal interlocuteur en ce qui concerne la sécurité de l’information au Collège et il relève de la Direction générale. 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.

Plus précisément, le RSI :

- élabore et propose le plan de sécurité de l’information du Collège en collaboration avec le comité chargé de la sécurité de l’information, rend compte de sa mise en œuvre à la Direction générale ;

- formule 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 et recommande les mises à jour de la Politique ;

- assure la coordination et la cohérence des mesures entreprises au sein du Collège en matière de sécurité de l’information et en conseillant les responsables d’actifs informationnels dans les directions et services ;

- produit les plans d’action, les bilans et les redditions de comptes du Collège en matière de sécurité de l’information ;

- propose des dispositions visant le respect des exigences en matière de sécurité de l’information à intégrer dans les ententes de service et les contrats ;

- s’assure, par l’intermédiaire du CSGI, de la déclaration par le Collège des risques et des incidents touchant la sécurité de l’information à portée gouvernementale au CERT/AQ ;

- collabore à l’élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l’information et veille au déploiement de ceux-ci ;

- procède aux enquêtes sur des transgressions sérieuses ayant trait présumément à la Politique après autorisation par la Direction générale ou le dirigeant de l’organisme ;

- s’assure des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l’évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l’information ;

- tient à jour le registre des dérogations et le registre des cas de contravention à la présente Politique.

Coordination sectorielle de la gestion des incidents (CSGI)

Outre sa participation active au réseau d’alerte gouvernemental, la coordination sectorielle de la gestion des incidents (CSGI) a notamment comme responsabilité :

- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l’information du Collège ;

- d’assurer la coordination des membres CERT/AQ qui lui sont rattachés et de mettre en œuvre les stratégies d’intervention appropriées ;

- de contribuer aux analyses de risques de sécurité de l’information, de recenser les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées ;

- de contribuer à la mise en œuvre du processus gouvernemental de gestion des incidents de sécurité de l’information ;

- d’élaborer et de tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications ;

- de collaborer étroitement avec le RSI et de lui fournir le soutien technique nécessaire à l’exercice de ses responsabilités.

Direction des finances et de l’approvisionnement

En qualité de responsable de la vérification interne, la Direction des finances et de l’approvisionnement joue un rôle clé dans la reddition de comptes en matière de sécurité de

l'information, plus particulièrement au regard du recensement, de l'évaluation et de la gestion des risques d'atteinte à la sécurité de l'information.

À ce titre, elle évalue, examine ou vérifie, entre autres :

- l'application, la validité et l'efficacité des règles, des mesures administratives et des moyens technologiques en matière de sécurité de l'information définis et mis en œuvre ;

- l'adéquation de l'intégration de la sécurité de l'information dans les processus opérationnels.

Direction des ressources humaines (DRH)

Dans la mise en œuvre de cette Politique, la Direction des ressources humaines (DRH) informe tout nouvel employé de ses obligations découlant de la présente Politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information et obtient son engagement à son respect, ce qui comprend l'engagement de confidentialité et le recensement de tels engagements.

De plus, la DRH :

- vérifie, au besoin, les antécédents des candidats à l'embauche et des membres du personnel concernés par la sécurité de l'information ;

- intervient auprès des membres du personnel concernés en cas d'atteinte à la sécurité des technologies de l'information, en collaboration avec le RSI et les autres intervenants ;

- informe les directions concernées d'une embauche, d'un changement de fonction et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels du Collège.

Elle met en œuvre, en collaboration avec le comité de sécurité de l'information, un programme institutionnel de formation et de sensibilisation en matière de sécurité de l'information.

Direction des ressources matérielles

La Direction des ressources matérielles participe, avec le RSI et le Service des affaires corporatives, à la détermination des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Collège, notamment en ce qui concerne les systèmes et les installations stratégiques ou des supports de l'information confidentielle.

Elle est également responsable de la gestion des accès physiques aux locaux du Collège et, à ce titre, elle s'assure de :

- mettre en place les mesures de protection physiques des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle ;

- sécuriser, gérer et contrôler les accès physiques (clés, cartes magnétiques, etc.) aux locaux et édifices du Collège ;

- concevoir et mettre en œuvre les mesures de protection physique des biens contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités du Collège ;

- en collaboration avec les directions ou services concernés, éliminer les supports de l'information de façon sécuritaire.

Service des ressources des technologies de l'information (SRTI)

En matière de sécurité de l'information, le Service des ressources des technologies de l'information (SRTI) s'assure de la prise en charge des exigences de sécurité de l'information numérique 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 établit et met en œuvre l'architecture décrivant la fonction, la structure et les interrelations des composantes de sécurité de l'information ;

- il arrime les solutions retenues aux processus organisationnels de sécurité de l'information ;

- il participe à la conception et à l'évaluation des composantes de sécurité de l'information des solutions d'affaires développées ou acquises par le Collège ;

- il coordonne l'élaboration du plan de continuité des services, veille à sa mise en œuvre et en assure la mise à jour ;

- il assure la planification et la coordination des tests initiaux et récurrents ;

- il applique des mesures d'intervention appropriées à toute menace ou à tout incident de sécurité de l'information, 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 est responsable du développement ou de l'acquisition de systèmes d'information, il conçoit, réalise et documente les fonctionnalités de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, à intégrer dans les systèmes d'information. Il s'assure également de leur bon fonctionnement ;

- il participe à la tenue des enquêtes relatives à des contraventions réelles ou apparentes à la présente Politique qui sont autorisées par la Direction générale.

Au-delà de son rôle habituel, la coordination du SRTI soutient également le RSI sur le plan tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de sécurité de l'information. Le SRTI soutient le RSI à plusieurs niveaux :

- dans la mise en œuvre des orientations internes découlant des directives gouvernementales, des politiques internes et des pratiques généralement admises à cet égard ;

- dans la production des bilans et des plans d'action de sécurité de l'information ;

- dans les négociations des ententes de service et des contrats et la formulation des recommandations quant à l'intégration de dispositions garantissant le respect des exigences de sécurité de l'information ;

- dans la tenue du registre des responsable de la gestion des accès.

Service des affaires corporatives

À titre de responsable de la gestion documentaire, le Service des affaires corporatives doit :

- 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 pour permettre une saine gestion des connaissances et du patrimoine informationnel, la préservation des preuves et le respect des lois ;

- collaborer étroitement avec les responsables d'actifs informationnels, ainsi qu'avec le RSI, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

Également, comme responsable de l'accès à l'information et de la protection des renseignements personnels, il 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 :

- communique au RSI les problèmes et les préoccupations de sécurité relativement à la protection des renseignements personnels ou sensibles ;

- contribue à assurer la cohérence et l'harmonisation des interventions avec 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 à portée gouvernementale.

Finalement, il veille à l'intégration de l'éthique aux processus de gestion de la sécurité de l'information, afin d'assurer la régularisation des conduites et la responsabilisation individuelle.

Responsables d’actifs informationnels

Les responsables d’actifs informationnels sont les membres du personnel cadre détenant l’autorité au sein des directions, des services, des centres d’études et des centres collégiaux de transfert de technologie, dont le rôle consiste à veiller à l’accessibilité, à l’utilisation adéquate et à la sécurité des actifs informationnels sous leur responsabilité. Le responsable d’actifs informationnels peut déléguer une partie de sa responsabilité.

Le responsable d’actifs informationnels :

- présente au personnel relevant de son autorité et les tiers avec lesquels il interagit, la politique sur la sécurité de l’information et des dispositions du cadre de gestion dans le but de s’assurer 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 sur la sécurité de l’information et de tout autre élément du cadre de gestion ;

- s’assure que les exigences en matière de sécurité de l’information sont prises en compte dans tout processus d’acquisition et tout contrat de 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 ;

- collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l’information ou à remédier à un incident de sécurité de l’information ainsi qu’à toute opération de vérification de la sécurité de l’information ;

- rapporte au RSI toute menace ou tout incident afférant à la sécurité de l’information ou tout problème lié à l’application de la présente Politique, y compris toute contravention réelle ou apparente d’un membre du personnel à ce qui a trait à l’application de cette Politique.

Personnes utilisatrices

La responsabilité de la sécurité de l'information du Collège incombe à toutes les personnes utilisatrices d'information et des actifs informationnels du Collège.

Toute personne utilisatrice qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'il en fait et doit agir de manière à protéger cette information.

À cette fin, la personne utilisatrice doit :

- prendre connaissance de la présente Politique et des directives et procédures qui en découlent ;
- utiliser les droits d'accès qui lui sont accordés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés ;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver ;
- signaler à son supérieur ou à son enseignant tout incident susceptible de constituer une contravention à la présente Politique ou de constituer une menace à la sécurité de l'information du Collège ou des gouvernements ;
- 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 ;
- se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister.

De plus, **la personne utilisatrice qui est membre du personnel doit** :

- si requis, participer à la catégorisation de l'information de son service ;
- s'engager par écrit à se conformer à certaines exigences légales, en particulier quant à la confidentialité ;

- au moment de son départ, qu'il soit temporaire ou définitif, et selon les procédures applicables, remettre les différentes cartes d'identité et d'accès, les clés, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à sa disposition dans le cadre de l'exercice de ses fonctions.

SANCTIONS

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

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente Politique et aux mesures de sécurité de l'information qui en découlent s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles disciplinaires internes applicables, y compris celles afférentes aux conventions collectives de travail et au Code de vie au Collège (règlement n^{o} 14).

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 Collège ou en vertu des dispositions de la loi applicable en la matière.

DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le RSI, assisté du comité chargé de la sécurité de l'information, est responsable de la diffusion et de la mise à jour de la Politique. La Politique sera révisée cinq ans après son adoption ou au besoin.

ENTRÉE EN VIGUEUR

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