Politique sur la sécurité de l'information
Numéro P-36

Adoption (instance/autorité)	*Date*	*Résolution*
Conseil d'administration	Le 1er mai 2019	C-4143-19
Modification (instance/autorité)	*Date*	*Résolution*
Abrogation (instance/autorité)	*Date*	*Résolution*

Entrée en vigueur	Le 1er mai 2019
Responsable de l'application	Direction générale
Historique	

TABLE DES MATIÈRES

1 ÉNONCÉ DE PRINCIPE

Dans l'accomplissement de sa mission, le Cégep de Matane doit protéger l'information qu'il a créée ou reçue et dont il est le gardien. Cette information est diversifiée et peut prendre différentes formes, notamment de renseignements personnels d'étudiants et de membres du personnel, d'information professionnelle sujette à des droits de propriétés intellectuelles ou de l'information stratégique ou opérationnelle utile à l'administration du cégep.

Dans ce contexte et avec l'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, chapitre. G-1.03* de même que de la *Directive sur la sécurité de l'information gouvernementale* émise par le Conseil du trésor, le cégep se dote d'une politique prévoyant des processus formels de sécurité de l'information.

La présente politique affirme l'engagement du cégep à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, le cégep doit veiller à :

- la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux 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 ;
- la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

La politique soutient la mise en œuvre du cadre de gestion en matière de sécurité de l'information et renforce le maintien de systèmes de contrôle interne offrant une assurance raisonnable de conformité à l'égard des lois, directives et pratiques gouvernementales en la matière.

2 CHAMP D'APPLICATION

La présente politique s'adresse à toute la communauté collégiale de même qu'à toute personne physique ou morale qui à titre de consultante ou consultant, de partenaire, de fournisseur ou de membre du public, utilise les actifs informationnels du cégep.

L'information et les actifs informationnels visés sont ceux que le cégep détient dans le cadre de ses activités, que leur conservation soit assurée par lui-même ou par un tiers, sur tout type de support.

3 DÉFINITIONS

La présente politique couvre les notions suivantes :

Actif informationnel

Une information, une banque d'informations, un système ou un support d'information. Un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le cégep habituellement accessible ou utilisable avec un dispositif des technologies de l'information (logiciels, progiciels, banques de données et d'information textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courriel électronique et système de messagerie vocale).

Cégep

Le Cégep de Matane.

CERT/AQ

Sigle issu des composants « Computer Emergency Response Team » et « administration québécoise», soit l'équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale.

CSGI

Coordonnatrice sectorielle ou coordonnateur sectoriel de gestion des incidents.

Plan de continuité

L'ensemble des mesures de planification établies et appliquées en vue de maintenir la disponibilité de l'information indispensable à la réalisation d'une activité au cégep.

Registre d'incident

Un recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, les mesures prises pour le rétablissement à la normale et le suivi.

RSI

Responsable de la sécurité de l'information.

Sécurité de l'information

La protection de l'information et des systèmes d'information contre les risques et les incidents.

4 DISPOSITIONS GÉNÉRALES

4.1 CADRE LÉGAL ET ADMINISTRATIF

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

- le cadre gouvernemental de gestion de la sécurité de l'information (juin 2014);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* (décret no 261-2012 du 28 mars 2012);
- la *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014);
- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, chapitre G-1.03*;
- la *Loi concernant le cadre juridique des technologies de l'information, RLRQ, chapitre C-1.1*;
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, chapitre A-2.1*;
- la *Loi sur les archives, RLRQ, chapitre A-21.1*;
- la *Loi sur le droit d'auteur, LRC (1985), chapitre C-42)*;

Cette politique est applicable en considérant les politiques, directives et guides du Cégep de Matane, soit :

- la *Politique relative à l'utilisation de la télématique du Cégep de Matane (P-29)*;
- la *Politique de gestion intégrée des documents (P-23)*;
- la *Politique de gestion de la propriété intellectuelle (P-18)*;
- la *Directive relative à la communication institutionnelle (D-6)*;
- le *Guide sur les médias sociaux* et la *nétiquette*.

4.2 PRINCIPES DIRECTEURS

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

- s'assurer de bien connaître l'information à protéger, en identifier les responsables et leurs caractéristiques de sécurité (principe qui confirme l'importance de maintenir à jour l'inventaire des actifs informationnels);
- informer la communauté collégiale des risques et des menaces pouvant affecter l'information afin que ses membres puissent reconnaître les incidents et les risques potentiels et comprendre leurs rôles et responsabilités en matière de sécurité de l'information en développant les habilités et les compétences appropriées;
- s'appuyer sur les normes pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires;
- adhérer à une approche basée sur le risque acceptable (la mise en place du cadre de gestion étant un moyen d'ajuster 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);
- reconnaître l'importance de la *Politique de sécurité de l'information* et du cadre de gestion de la sécurité de l'information qui doivent être articulés par une équipe compétente et suffisante en nombre (cette équipe devant définir, mettre en place, opérer et ajuster la gestion de la sécurité de l'information);
- protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;
- reconnaître que l'environnement technologique est en changement constant et interconnecté avec le monde (en mettant en place une gestion de la sécurité de l'information qui s'adapte à ces changements);
- reconnaître l'importance d'évaluer régulièrement 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 actions d'éradication des menaces ou de recouvrement des activités compromises;
- protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction (le niveau de sécurité pouvant varier au cours du cycle de vie du document);
- adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de la sécurité de l'information avec le réseau de l'éducation et organismes publics;
- adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle (chaque individu qui a accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci);
- s'assurer que chaque membre du personnel a accès au minimum d'information requis pour accomplir ses tâches normales;
- mettre en place un plan de continuité en vue de rétablir les services essentiels à sa clientèle, selon un temps prévu.

4.3 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 cégep par la mise en place d'un cadre de gestion de la sécurité permettant notamment une reddition de comptes adéquate.

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

La *Politique de sécurité de l'information* du cégep s'articule autour de trois axes fondamentaux de gestion, soit la gestion des accès, la gestion des risques et la gestion des incidents.

4.3.1 Gestion des accès

La gestion des accès doit être encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le dessein de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité des personnes, à tous les niveaux de personnel du cégep.

4.3.2 Gestion des risques

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du cégep. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du cégep. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Le niveau de protection de l'information est établi en fonction :

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

4.3.3 Gestion des incidents

Le cégep déploie des mesures de sécurité de l'information afin d'assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires afin de :

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

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

Dans la gestion des incidents, le cégep peut exercer ses pouvoirs et ses prérogatives eu égard à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

4.4 SANCTIONS

En cas de contravention à la présente politique, l'utilisatrice ou l'utilisateur engage sa responsabilité personnelle. Il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

Toute ou 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, dont celles de conventions collectives de travail et du *Code de conduite du Cégep de Matane (R-13)*.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, une ou un partenaire, une ou un invité, une consultante ou un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au cégep ou en vertu des dispositions de la législation applicable en la matière.

5 RESPONSABILITÉS

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

Conseil d'administration

Le conseil d'administration adopte la *Politique de sécurité de l'information* ainsi que toute modification à celle-ci. Le conseil est régulièrement informé des actions du cégep en matière de sécurité de l'information.

Direction générale

La directrice générale ou le directeur général veille à l'application de la *Politique sur la sécurité de l'information* et a pour tâche :

- d'encadrer la ou le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat;
- de déléguer certaines responsabilités à la secrétaire générale ou au secrétaire général pour la gestion de l'information;
- de faire adopter par le conseil d'administration les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information;
- d'autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission du cégep;
- d'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique;
- de tenir à jour le registre des dérogations et le registre des cas de contravention à la présente politique.

Responsable de la sécurité de l'information (RSI)

La fonction de la ou du RSI est déléguée à un membre du personnel cadre par le conseil d'administration. La ou le RSI relève de la directrice générale ou du directeur général au sens du cadre gouvernemental de gestion de la sécurité de l'information. Cette personne met en place le cadre de gestion de la sécurité de l'information et s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins.

Plus spécifiquement, il a pour tâche :

- d'élaborer et de proposer le cadre de gestion de sécurité de l'information du cégep ainsi que de rendre compte de son implantation au comité de direction;
- de 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 et de mettre à jour la politique;
- d'assurer la coordination et la cohérence des actions menées au sein du cégep en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans les unités;
- de produire les plans d'action, les bilans et les redditions de comptes du cégep en matière de sécurité de l'information;
- de proposer des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;

- de s’assurer de la déclaration des risques et des incidents de sécurité de l’information à portée gouvernementale (CERT/AQ);
- de collaborer à l’élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l’information et de veiller au déploiement de ceux-ci;
- de procéder aux enquêtes relatives à des transgressions réelles ou présumées ayant trait politique à la suite de l’autorisation du dirigeant de l’organisme;
- d’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.

Coordonnatrice sectorielle ou coordonnateur sectoriel de gestion des incidents (CSGI)

La coordonnatrice sectorielle ou le coordonnateur sectoriel de gestion des incidents (CGSI) représente le cégep en matière de déclaration des incidents à portée gouvernementale de la sécurité de l’information. La ou le RSI désigne les personnes agissant à titre de CGSI au cégep. Ce dernier à la responsabilité :

- de participer activement au réseau alerte gouvernemental
- d’assurer le relais entre le cégep et le CERT/AQ et de mettre en œuvre les stratégies de réaction appropriées;
- de déclarer les incidents au CERT/AQ;
- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l’information au cégep;
- de contribuer aux analyses de risques de sécurité de l’information, d’identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
- de seconder la ou le RSI.

Secrétaire générale ou secrétaire général

En sa qualité de responsable des archives, de l’accès aux documents et de la protection des renseignements personnels, la secrétaire générale ou le secrétaire général agit comme personne-ressource pour toute question ou problématique relative à la sécurité des renseignements personnels à l’égard des documents, à l’application de telles mesures et à ce que des correctifs soient apportés, le cas échéant.

Responsable d’actifs informationnels

La ou le responsable d’actifs informationnels est le membre du personnel cadre détenant l’autorité au sein d’un service, qu'elle soit d’ordre pédagogique ou d’ordre administratif, et dont le rôle consiste à veiller à l’accessibilité, à l’utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il peut donc y avoir plusieurs responsables d’actifs informationnels dans un cégep. Ce dernier peut déléguer la totalité ou une partie de ses responsabilités à une ou un autre membre du service, soit :

- informer le personnel relevant de son autorité et les tiers avec lesquels transige le service de la *Politique de sécurité de l’information* et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s’y conformer;
- collaborer activement à la catégorisation de l’information du service sous sa responsabilité et à l’analyse de risques;
- voir à la protection de l’information et des systèmes d’information sous sa responsabilité et veiller à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la *Politique de sécurité de l’information* et de tout autre élément du cadre de gestion;
- s’assurer 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 voir à ce que toute ou tout consultant, fournisseur, partenaire, invitée ou invité, organisme ou firme externe s’engage à respecter la politique et tout élément du cadre de gestion;
- rapporter au Service des ressources informationnelles toute menace ou tout incident afférant à la sécurité de l’information;

- 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 ;
- rapporter à la directrice générale ou au directeur général tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

Comité de travail sur la sécurité de l'information

Le comité de travail pour la sécurité de l'information est un comité chargé d'assister la ou le responsable de la sécurité de l'information (RSI) durant la mise en place du cadre de gestion, des plans d'action, des bilans de sécurité de l'information, des activités de sensibilisation ou de formation ainsi que de toute autre proposition d'action en matière de sécurité de l'information. Ce comité est formé de différents corps d'emploi du cégep qui participent à la mise en place de la sécurité de l'information. Il constitue également un forum d'échange actif tout au long de l'évolution du projet.

Service des ressources informationnelles

En matière de sécurité de l'information, le Service des ressources informationnelles s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels il intervient. Son rôle est de :

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

Service des ressources matérielles

Le Service des ressources matérielles participe, avec la ou le responsable de la sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du cégep.

Utilisateurs

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs qui accèdent à une information, qui la consultent ou qui la traitent.

À cette fin, l'utilisatrice ou l'utilisateur doit :

- prendre connaissance de la politique et y adhérer en la respectant;
- se conformer à la présente politique et à toute autre directive du cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- participer à la catégorisation de l'information de son service;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- signaler à la ou au responsable des actifs informationnels de son unité ou à la ou au responsable de la sécurité de l'information tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du cégep;
- collaborer à toute intervention visant à indiquer ou à mitiger une menace à la sécurité de l'information ou un incident de sécurité de l'information.

6 ENTRÉE EN VIGUEUR ET DIFFUSION

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration. Elle est diffusée par le Secrétariat général.

7 CALENDRIER DE RÉVISION

Cette politique peut être révisée à tout moment. Toutefois, une révision est prévue cinq (5) ans à compter de la date de son adoption.

8 MODIFICATIONS MINEURES

Toute modification mineure peut être effectuée par la secrétaire générale ou le secrétaire général qui en informe le comité de direction. Est considérée mineure toute modification au nom d'une direction ou d'un service, au titre d'un document officiel, au nom du poste d'une ou d'un titulaire, au numéro d'un article, à la mise en page ou à une délégation de pouvoir effectuée par le conseil d'administration.