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*
Conseil d'administration	Le 17 juin 2026	C-4889-26
Abrogation (instance/autorité)	*Date*	*Résolution*

Entrée en vigueur	Le 17 juin 2026
Responsable de l'application	Direction générale

Historique

Juin 2026 : refonte majeure de la politique pour intégrer les exigences de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ 2021, c. 25), de la *Directive sur la sécurité de l'information gouvernementale* (2021) et de l'*Arrêté ministériel MCN-AN 2024-05 concernant le Modèle de classification de sécurité des données numériques gouvernementales*. Restructuration du cadre de gestion autour de six principes directeurs alignés sur le *NIST Cybersecurity Framework* et révision des rôles et responsabilités (introduction des fonctions de personne CSIO et COMSI).

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 de personnes étudiantes 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 modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c 25,* 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*, la *Directive sur la sécurité de l'information gouvernementale* émise par le Conseil du trésor, de même que l'Arrêté numéro MCN-AN 2024-05 du 12 décembre 2024 de la part du ministre de la Cybersécurité et du Numérique concernant le Modèle de classification de sécurité des données numériques gouvernementales, 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 qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- L'intégrité de l'information de manière 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 du Cégep de Matane, de même qu'à toute personne physique ou morale qui, à titre de personne consultante, 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.

COMSI

Coordination organisationnelle des mesures de sécurité de l'information.

Personne CSIO

Personne Cheffe de la Sécurité de l'information (CSIO).

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.

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 présente politique 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 1514-2021 du 8 décembre 2021);
- 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 (chapitre A-21.1)*;
- La *Loi sur le droit d'auteur, LRC (1985), chapitre C-42)*;
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, LQ 2021, c 25 (septembre 2021)*;
- L'*Arrêté ministériel concernant le Modèle de classification de sécurité des données numériques gouvernementales lq 2021 (décembre 2024)*.

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*.

Tout en étant adaptés au contexte règlementaire du Québec et opérationnel du cégep, les principes directeurs et piliers de la sécurité de la présente politique de sécurité de l'information s'inspirent des normes ci-après :

- *Nist Cybersecurity Framework (CSF);*
- *NIST SP 800-53 Rev 5.*

4.2 PRINCIPES DIRECTEURS ET APPROCHES DE GESTION

4.2.1 Principes directeurs

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

4.2.1.1 Structurer la gouvernance de la sécurité de l'information

Le cégep se donne comme ambition de renforcer sa politique de sécurité de l'information, ses procédures et processus opérationnels de sécurité.

Cette approche comprend notamment :

- Une application rigoureuse des exigences légales, politiques institutionnelles en vigueur et des normes pertinentes afin de favoriser le déploiement des meilleures pratiques en matière de sécurité de l'information;
- Un recours à l'audit et aux barèmes de comparaison avec des organismes ou établissements similaires pour améliorer ses capacités;
- Une mise en application de la politique par une équipe compétente et suffisante en nombre;
- Une meilleure définition des rôles et responsabilités en matière de sécurité de l'information pour l'ensemble de la communauté collégiale;
- Une adhésion aux principes de partage des meilleures pratiques et informations opérationnelles de sécurité de l'information avec le réseau de l'éducation et les organismes publics.

4.2.1.2 Identifier les actifs et gérer les risques

Le cégep se donne comme ambition de mieux identifier, classifier et gérer ses actifs informationnels et ses dépendances, tout en identifiant leur risque de sécurité de manière rigoureuse, en s'appuyant sur des processus structurés.

Cette approche comprend notamment :

- Une bonne connaissance du contexte du cégep, c'est-à-dire sa mission, ses objectifs, son activité, ses parties prenantes, son environnement réglementaire et légal, ses ressources et capacités pour prioriser ses efforts de sécurisation de l'information;
- Une bonne connaissance de son patrimoine informationnel (information ou actif informationnel) à protéger;
- Une identification des dépendances des services offerts à la communauté collégiale qui s'appuieraient sur des fournisseurs, des infrastructures partagées ou des systèmes interconnectés.

4.2.1.3 Renforcer la protection des actifs

Le cégep se donne comme ambition de mettre en œuvre les mesures appropriées pour prévenir, atténuer et maîtriser les effets d'un incident de sécurité de l'information.

Cette approche comprend notamment :

- Une protection rigoureuse des renseignements personnels et de toute autre information sensible contre toute divulgation, indisponibilité et modification ou suppressions non autorisées;
- Une sécurisation de l'information tout au long de son cycle de vie, de sa collecte ou création jusqu'à sa destruction, en mettant en œuvre des technologies de protection adéquates à chaque étape;
- Une limitation des accès au minimum d'information requis pour accomplir ses tâches normales;
- Une implication de la communauté collégiale à la sécurisation par la formation et la sensibilisation sur les risques et les menaces pouvant affecter l'information;
- Une adhésion à la démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

4.2.1.4 Améliorer la détection des incidents et des anomalies

Le cégep se donne comme ambition de mettre en place et de maintenir un dispositif de signalement, d'identification et de suivi des incidents de sécurité.

Cette approche comprend notamment :

- La définition et la documentation des opérations dans un fonctionnement normal des ressources informationnelles du cégep;
- La surveillance permanente des ressources informationnelles pour détecter et tracer les évènements de sécurité et s'assurer ainsi du bon fonctionnement des contrôles de sécurité;
- L'analyse des évènements issus des ressources informationnelles pour en déceler les éventuelles anomalies;
- La mise en place et la vérification régulière de processus et de procédures de détection.

4.2.1.5 Répondre efficacement face aux incidents

Le cégep se donne comme ambition de mettre en place et de maintenir un dispositif de réaction efficace, de résolution et de traçabilité des incidents de sécurité.

Cette approche comprend notamment :

- La mise en place un plan de réponse aux incidents en vue de rétablir les services essentiels, selon un temps prévu;
- La formation des parties prenantes impliquées aux processus et procédures et la réalisation d'exercice régulier pour s'assurer d'une réponse coordonnée;
- La définition des canaux de communication pour informer la communauté collégiale pendant et après un incident;
- L'application de mesures concrètes visant à atténuer l'impact des incidents et à en faciliter la résolution.

4.2.1.6 Restaurer ses capacités et ses services

Le cégep se donne comme ambition de restaurer ses capacités et ses services en cas de survenance d'un incident ou d'un sinistre.

Cette approche comprend notamment :

- La mise en place et la révision de processus et procédures pour assurer la restauration rapide des ressources informationnelles affectées par un incident de sécurité de l'information;
- La définition de canaux de communication pour coordonner les actions de récupération par les parties prenantes, à l'interne du cégep comme à l'externe;
- La réalisation d'une analyse post-mortem des activités de récupération et la documentation des interventions pour améliorer les actions futures.

4.2.2 Classification et gestion des actifs informationnels

Le cégep procède à l'inventaire et la documentation de l'ensemble de ses ressources informationnelles, ses services essentiels, incluant les propriétaires de ses actifs. La classification des actifs informationnels est en quatre (4) niveaux, selon le niveau de préjudice aux personnes physiques ou morales, à la communauté collégiale, à l'institution du cégep ou à la province de Québec qu'entrainerait la divulgation, l'indisponibilité, la modification ou l'altération de l'information :

- **Secret** : préjudice élevé ou très élevé;
- **Restreint** : préjudice modéré;
- **Interne** : préjudice faible;
- **Public** : préjudice très faible.

Le cégep s'assure qu'à chaque niveau de classification, correspondent des contrôles de sécurité de base (minimal) à mettre en place.

4.2.3 Gouvernance

Le cégep établit une gouvernance de la sécurité de façon efficace pour garantir la sécurité de l'information et la protection des renseignements personnels. Cette gouvernance est alignée avec les objectifs stratégiques du Cégep de Matane. Le cégep s'assure d'actualiser sa pratique de sécurité en intégrant les nouvelles exigences légales, réglementaires, normatives et corporative éprouvées.

Les instances de pilotage de la sécurité du cégep, ainsi que les rôles et des responsabilités, sont identifiés et attribués clairement pour garantir une mise en place et une efficacité des contrôles de sécurité de l'information.

4.2.4 Gestion des identités et des accès

La gestion des accès est encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées (besoin d'en connaitre) et repose sur la *Directive de gestion des identités et des accès (D-28)*. 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 principalement sur :

- L’attribution de responsabilités et une imputabilité des personnes, à tous les niveaux de personnel du cégep;
- La gestion du cycle de vie des comptes, y compris la création, la modification, la désactivation et la suppression;
- La mise en œuvre des mécanismes de restriction d’accès aux informations et aux ressources basées sur le rôle et des attributs;
- La séparation des tâches et la limitation des accès privilégiés aux personnes autorisées;
- La gestion sécurisée des informations d'authentification, tels que les mots de passe, pour assurer leur sécurité.

4.2.5 Sensibilisation et formation à la sécurité

Le cégep s’assure que la communauté collégiale soit formée et sensibilisée aux enjeux de sécurité. Pour ce faire, le cégep met en place et maintient un dispositif d’information et de formation à la sécurité de l’information, destiné de l’ensemble de la communauté collégiale.

4.2.6 Gestion des fournisseurs et des services externalisés

Les exigences en matière de sécurité de l’information du cégep sont intégrées dans les ententes réalisées avec les tiers. Le cégep s’assure de rester en maitrise des risques liés à l’externalisation de ses services notamment infonuagiques.

Ainsi, l’origine et les personnes responsables des modifications, ou changements à apporter aux ressources informationnelles par un tiers, sont documentés et surveillés.

Les fournisseurs et les services externalisés sont régulièrement évalués pour s’assurer du respect dans le temps des clauses contractuelles.

4.2.7 Sécurité des systèmes, de l’infrastructure et des communications

Le cégep met en place les mesures nécessaires pour assurer l’intégrité et la confidentialité des informations communiquées. De plus, le cégep met également en place les mesures nécessaires pour garantir la disponibilité des systèmes en charge de cette communication.

4.2.8 Sécurité physique et environnementale

Le cégep identifie et prévient les accès non autorisés à ses installations physiques, principalement aux zones les plus sensibles de son espace (ex. zones où sont emmagasinés les informations, les services ou systèmes les plus sensibles).

Ainsi le cégep s’assure notamment de mettre en place :

- Des restrictions aux seules personnes autorisées, l’accès physique aux installations contenant des ressources informationnelles importantes (ex. salle des serveurs, etc.);
- Une surveillance des entrées et sorties des installations;
- Des mesures de surveillance contre les menaces environnementales.

4.2.9 Gestion des incidents, de la continuité et de la reprise

Le cégep met en place et maintient un dispositif de signalement, d'identification, de traitement et de suivi des incidents de sécurité.

Le cégep déploie également des mesures de sécurité de l'information afin d'assurer la continuité de ses services.

À cet effet, le cégep s'assure notamment de mettre en place :

- Des rôles et responsabilités clairement définis quant à la prise en charge des incidents de sécurité;
- Un comité de coordination des mesures d'urgence;
- Une capacité opérationnelle pour répondre et limiter l'occurrence des incidents en matière de sécurité de l'information ;
- Une gestion adéquate de ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Dans l'éventualité d'un sinistre ou d'un incident majeur, le cégep s'assure de l'anticiper en mettant en place les moyens de poursuivre au mieux ses activités courantes.

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.

4.2.10 Évaluation et amélioration continues

Conformément aux normes et procédures afférentes, le cégep évalue régulièrement ses contrôles de sécurité afin de s'assurer de maintenir un niveau de sécurité acceptable et d'améliorer en continu ses contrôles.

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.

4.3 SANCTIONS

En cas de contravention à la présente politique, la personne utilisatrice 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 personne 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 personne invitée, une personne consultante 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 présente politique 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 Direction générale veille à l'application de la présente politique et a pour tâche :

- D'encadrer la personne Cheffe de la sécurité de l'information (CSIO) dans la réalisation de son mandat;
- D'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la présente politique.

Personne Cheffe de la Sécurité de l'information (CSIO)

La fonction de la personne Cheffe de la Sécurité de l'information (CSIO) est déléguée à une personne membre du personnel cadre par le conseil d'administration. Cette personne s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins. Plus spécifiquement, elle a pour tâche :

- De faire adopter par le conseil d'administration les orientations stratégiques, les plans d'action, les bilans de sécurité et les redditions de comptes en matière de sécurité de l'information;
- 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 présente 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;
- 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;
- De tenir à jour le registre des dérogations à la présente politique ou aux directives en découlant;
- De procéder aux enquêtes relatives à des transgressions réelles ou présumées ayant trait à la présente 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.

Personne responsable de la coordination organisationnelle des mesures de sécurité de l'information (COMSI)

La personne responsable de la coordination organisationnelle des mesures de sécurité de l'information (COMSI) au cégep, désignée par la personne CSIO, représente le cégep en matière de déclaration des incidents à portée gouvernementale de la sécurité de l'information. Elle a la responsabilité :

- De participer activement au réseau d'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 personne CSIO.

Personne détentrice d'information

Les personnes détentrices de l'information sont désignées par la personne CSIO. Leurs noms et les systèmes d'information qui leur sont assignés sont consignés au registre d'autorité. Toute personne détentrice de l'information a la responsabilité de :

- Participer à l'élaboration des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans en matière de sécurité de l'information;
- Catégoriser l'information relevant de sa responsabilité en fonction de sa valeur et selon les critères de disponibilité, d'intégrité et de confidentialité;
- Veiller à ce que les mesures de sécurité de l'information adoptées soient mises en place et appliquées et qu'elles répondent adéquatement aux risques encourus, incluant la gestion des accès;
- Agir comme maître d'œuvre des analyses de risques et s'assurer de la prise en charge des risques résiduels;
- Veiller au respect du registre d'autorité par les personnes utilisatrices qui relèvent de sa responsabilité.

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;
- D'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;
- De participer à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la Direction générale.

Service des ressources matérielles

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

Personnes utilisatrices

La responsabilité de la sécurité de l'information incombe à toutes les personnes utilisatrices qui accèdent à une information, qui la consultent ou qui la traitent.

À cette fin, la personne utilisatrice doit :

- Prendre connaissance de la présente politique et des différentes directives en découlant, 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 ainsi que 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 sa personne gestionnaire, à la personne COMSI ou CSIO, 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 personne CSIO ou par le Secrétariat 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.