CÉGEP SAINT-JEAN-SUR-RICHELIEU

Politique de sécurité de l'information

Direction des technologies de l'information

Adoptée par le Conseil d'administration le 20 septembre 2022
Résolution : 2022-CA07-07

Table des matières

PRÉAMBULE

La Politique de sécurité de l'information établit les balises nécessaires à la protection des différents actifs informationnels détenus par le Cégep Saint-Jean-sur-Richelieu dans le cadre de ses différentes activités. Le Cégep reconnaît que l'information est essentielle à ses opérations courantes et qu'elle doit donc faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate. Il s'agit, notamment, des renseignements personnels des étudiant.es, des membres du personnel et de tierces parties, d'information professionnelle sujette à des droits de propriété intellectuelle et d'informations stratégiques ou opérationnelles utilisées pour l'administration du Collège.

1. DÉFINITIONS ET ABRÉVIATIONS

Actif informationnel : Une information, une banque d'information, 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, didacticiels, banques de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

Catégorisation : Processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information et, conséquemment, le niveau de protection à lui accorder en matière de disponibilité, d'intégrité et de confidentialité.

COCD : Centre opérationnel de cyberdéfense du Ministère de l'Éducation et de l'Enseignement supérieur. Les centres des différents ministères et organismes publics sont supervisés par le Centre gouvernemental de cyberdéfense.

COMSI : Coordonnatrice organisationnelle ou coordonnateur organisationnel des mesures de sécurité de l'information.

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées, les ayants droit.

CSIO : Chef de la sécurité de l'information organisationnelle.

Cycle de vie de l'information : Ensemble des étapes que franchit une information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction en conformité avec le calendrier de conservation du Cégep Saint-Jean-sur-Richelieu.

DSIG : Directive sur la sécurité de l'information gouvernementale.

Responsable d'actif informationnel : Membre du personnel d'encadrement détenant la plus haute autorité au sein d'une unité pédagogique ou administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité.

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

Incident : Un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

Intégrité : Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

Plan de relève : Plan de reprise hors site mis en œuvre lorsqu'il y a détérioration ou destruction d'actifs informationnels consécutive à un incident exigeant le transfert de l'exploitation dans un autre lieu ou une autre salle des serveurs. Le plan de relève décrit les procédures visant à assurer, dans des conditions de continuité adaptées à l'urgence de la situation.

Plan de continuité : Ensemble de mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation des activités régulières du Cégep.

DTI : Direction des technologies de l'information.

Utilisatrice et utilisateur : Tout le personnel, toute personne physique ou morale qui, à titre d'employé.e, d'étudiant.e, de consultant.e, de partenaire, de fournisseur ou d'invité.e, utilise les actifs informationnels du Cégep.

2. CADRE LÉGAL

Le Cégep Saint-Jean-sur-Richelieu, en sa qualité d'organisme public, est soumis à plusieurs directives, lois ou règlements émis par le gouvernement du Québec.

Ainsi, la Politique de sécurité de l'information s'inscrit principalement dans un contexte régi par les lois et documents suivants :

- la *Charte des droits et libertés de la personne* (LRQ, chapitre C-12);
- le *Code civil du Québec* (LQ, 1991, chapitre 64);
- 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* (LGGRI-- LRQ, chapitre G-1.03, amendée en 2017);
- la *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
- la *Politique gouvernementale de cybersécurité* (SCT, 2020);
- 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, 1985, chapitre C-46);
- le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*;

- la Directive sur la sécurité de l'information gouvernementale (DSIG);
- la *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42).

3. CHAMP D'APPLICATION

La présente politique s'adresse aux personnes utilisatrices, c'est-à-dire à tous les membres du personnel, peu importe leur statut, et à toute personne physique ou morale qui, à titre d'employé.e, d'étudiant.e, de partenaire, de consultant.e, d'invité.e ou de fournisseur, utilise les actifs informationnels du Collège ou y a accès ainsi qu'à toute personne qui est dûment autorisée par le Cégep à y avoir accès, et ce, dans le respect des lois en vigueur et du cadre réglementaire qui régit le Cégep.

L'information visée par la politique est celle que le Cégep détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers. Tous les supports, numériques et incluant le papier, sont concernés.

4. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Collège 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 Collège doit veiller à :

- Assurer la disponibilité de l'information de manière qu'elle soit accessible en temps voulu et de la façon requise aux personnes autorisées par le Collège.
- L'intégrité de l'information de manière à ce qu'elle ne soit ni altérée, ni détruite d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues.
- Assurer la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seuls ayants droit, principalement s'il s'agit de renseignements personnels ou sensibles.

Par conséquent, le Cégep met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera précisée par le biais du Cadre de gestion de la sécurité de l'information du Collège.

Cette politique jumelée avec le Cadre de gestion de la sécurité de l'information renforcera les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins du Cégep en matière de réduction du risque associé à la protection de l'information.

5. 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 en lien avec l'inventaire des actifs informationnels.
- Adopter une approche basée sur le risque acceptable permettant de garantir la sécurité de l'information tout au long de son cycle de vie.

- Maintenir un équilibre entre l'accès aux outils permettant de fournir la prestation de travail et la sécurité de l'information.
- Maintenir à jour le Cadre de gestion de la sécurité de l'information afin notamment d'encadrer l'utilisation des actifs informationnels par les utilisateurs.
- Réévaluer régulièrement les risques, mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information.
- Identifier, réduire et contrôler les risques pouvant porter atteinte aux informations ou aux systèmes d'information du Cégep.
- Adhérer aux principes de partage des meilleures pratiques en matière de la sécurité de l'information avec le réseau de l'éducation et des organismes publics.
- Reconnaître que l'efficacité des mesures de sécurité de l'information repose entre autres sur l'attribution de responsabilités et sur l'imputabilité des personnes utilisatrices.
- S'assurer que chaque employé.e doit avoir accès au minimum d'information requise pour accomplir ses tâches normales.
- Mettre en place un plan de continuité des affaires ou de relève adapté au niveau de gravité de l'incident en cybersécurité ou du sinistre selon le cas.

6. DISPOSITIONS GÉNÉRALES ET PARTICULIÈRES D'APPLICATION

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 Saint-Jean-sur-Richelieu s'articule autour de trois axes fondamentaux de gestion en matière de sécurité de l'information. Ces axes sont :

- la gestion des accès;
- la gestion des risques;
- la gestion des incidents.

7. 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 par le Collège. Ces mesures sont prises essentiellement afin de protéger l'intégrité et la confidentialité des données et des renseignements personnels et de toutes données sensibles de l'organisation.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité de tous les membres du personnel et sur l'obligation pour chaque membre d'en rendre compte selon leur fonction au sein du Collège.

La gestion des accès est un enjeu important au Cégep Saint-Jean-sur-Richelieu, il fera l'objet d'un processus de gestion spécifique dans le Cadre de gestion de la sécurité de l'information et d'une directive en Gestion des identités et des accès (GIA).

8. 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 et d'y appliquer des mesures à la hauteur du niveau de sensibilité de l'information.

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 Collège. Les risques à portée gouvernementale seront 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'incident, d'erreur ou de malveillance auxquelles elle est exposée;
- des conséquences de la réalisation de ces risques;
- du niveau de risque acceptable par le Cégep.

9. GESTION DES INCIDENTS

Le Cégep déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, le Collège met en place de façon proactive les mesures suivantes :

- Rechercher, corriger et réduire les vulnérabilités de l'organisation face aux menaces en matière de sécurité de l'information en appliquant les bonnes pratiques en cette matière.
- Gérer adéquatement les incidents afin de minimiser les conséquences et rétablir les activités et les opérations.
- Mettre en place des mesures correctives lors d'un incident afin de rétablir les services affectés et éviter les impacts sur les utilisatrices et utilisateurs.
- Déclarer les incidents de sécurité de l'information à portée gouvernementale au Centre opérationnel en cyberdéfense (COCD) du Ministère de l'Enseignement supérieur conformément à la DSIG et à la Politique gouvernementale en cybersécurité.
- Exercer ses pouvoirs et ses prérogatives à l'égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

10. RÔLES ET RESPONSABILITÉS

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents responsables du Cégep. La mise en place d'un Cadre de gestion de la sécurité de l'information permettra d'apporter des précisions sur les différents mécanismes et mesures à mettre en place afin d'assurer la sécurité optimale de l'information tout au long de son cycle de vie.

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 occupent.

10.1 Conseil d'administration

Le Conseil d'administration adopte la Politique de sécurité de l'information ainsi que toute modification éventuelle à celle-ci.

10.2 La Direction générale

La Direction générale est la première responsable organisationnelle de la sécurité de l'information et assure la mise en œuvre et les suivis découlant de la présente politique.

La Direction générale verra à :

- Encadrer la personne chef de de la sécurité de l'information organisationnel (CSIO) dans la réalisation de son mandat.
- 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.
- Autoriser une enquête lors d'une transgression de la politique.

10.3 Comité de la sécurité de l'information (CSI)

Ce comité de travail sous la responsabilité de la ou du CSIO a un rôle tactique au niveau de la sécurité de l'information du Collège et en lien avec le Plan des mesures d'urgence (PMU) du Collège. Ce comité est composé de personnel d'encadrement de l'organisation et se prononce sur les mesures et autres éléments pouvant être nécessaires afin d'assurer la sécurité de l'information du Cégep et être conforme à la réglementation. Il travaillera en collaboration avec la DTI à la préparation des plans de continuité et de relève du Cégep. Ce comité aura comme mandat de définir les types d'incidents potentiels et à définir et planifier les actions à entreprendre en fonction du niveau de gravité de chacun. Il sera également appelé à se réunir en urgence et intervenir rapidement en cas de tentatives d'intrusions ou d'incidents portant atteinte à la sécurité informationnelle du Collège. En cas d'urgence à la suite d'un incident majeur, le comité assurera la coordination des actions et des rôles de chaque intervenant.e qui est en mesure de contribuer au rétablissement de l'offre de service régulière du Collège. Le comité verra à maintenir une liste de contacts d'organismes pouvant offrir une aide ponctuelle en situation de crise et qui pourraient permettre une intervention rapide afin de réduire les impacts au niveau des services du Collège. À titre d'exemples, la personne responsable du volet sécurité informationnelle à la Fédération des cégeps et la personne-ressource chez

l'assureur du risque en sécurité de l'information seront notamment des membres collaborateurs de première ligne.

Ce comité devrait faire partie du PMU (Plan des mesures d'urgence du Cégep) et à ce titre, la ou le CMU (coordonnatrice ou coordonnateur des mesures d'urgence du Cégep) sera membre de ce comité d'office. La directrice ou le directeur des études, la ou le DSA, la ou le gestionnaire au Service des communications, la ou le CSIO et la ou le COMSI devraient en assurer la composition. Le comité sera responsable de préparer un plan de communication selon le niveau de gravité de l'incident. Le registre des incidents en cybersécurité tenu à jour par la ou le COMSI pourra alimenter les actions du comité.

Au besoin, la Direction générale participera aux travaux du comité dans le cas d'incidents majeurs en sécurité de l'information. Elle sera également informée des décisions du comité ayant un impact sur l'offre de services du Collège et devra y donner son aval avant d'appliquer les recommandations du CSI.

10.4 Comité consultatif de la sécurité de l'information (CCSI)

Ce comité de travail également sous la responsabilité de la personne CSIO a comme objectif de participer à l'élaboration de la présente politique de la sécurité de l'information. Ce comité a un mandat de nature opérationnelle.

Il est consulté sur les activités de sensibilisation ou de formation ainsi que toutes propositions d'action en matière de sécurité de l'information qui touche la communauté collégiale. C'est aussi un forum d'échange entre les parties prenantes et d'observation du déploiement de la présente politique et du Cadre de gestion de la sécurité de l'information.

Ce comité sera composé d'un maximum de dix personnes. En plus de la personne CSIO et de la ou le COMSI, le comité sera formé de la directrice ou directeur de la Formation continue, de la ou le gestionnaire aux Affaires corporatives, d'un.e gestionnaire de la D-É (bibliothèque), de la personne qui coordonne le Département de l'informatique et des représentant.es des syndicats du Collège et d'un.e étudiant.e.

10.5 Chef de la sécurité de l'information organisationnelle (CSIO)

La fonction de la personne CSIO est déléguée à un.e cadre par le conseil d'administration du Collège. La personne CSIO relève de la Direction générale au sens du Cadre gouvernemental de gestion de la sécurité de l'information. Idéalement, elle devrait être la directrice ou le directeur de la DTI.

Cette personne participe activement à l'élaboration et au déploiement de la présente politique et du 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 du Collège soit en adéquation avec ceux-ci.

La personne CSIO assume les responsabilités suivantes :

- En collaboration avec les deux comités de travail sous sa responsabilité, soumettre à la Direction générale les orientations, les directives, les modifications au Cadre de gestion de la sécurité de l'information, les priorités d'action, les éléments de reddition de comptes ainsi que tout incident ayant mis ou qui aurait pu mettre en péril la sécurité de l'information de son organisation.

- Assurer, en collaboration avec la ou le COMSI, 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 services et en leur offrant de la formation si nécessaire.
- 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.
- Collaborer à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information du Cégep et veiller au déploiement de ceux-ci.
- Procéder aux enquêtes dans des transgressions sérieuses ayant trait à la présente politique à la suite de l'autorisation de la Direction générale.
- S'assurer des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des standards, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.
- Formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation afin de préserver les actifs informationnels du Cégep en cas d'urgence.
- S'assurer de la contribution du Collège au processus de gestion des incidents de sécurité à portée gouvernementale, et ce, en collaboration avec la ou le COMSI.
- Tenir à jour le registre des dérogations et le registre des cas de contraventions à la présente politique.

10.6 Coordonnatrice organisationnelle ou coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

La ou le COMSI apporte son soutien à la personne CSIO du Cégep, notamment en ce qui a trait à la gestion des incidents et des risques en sécurité de l'information. Cette personne est l'interlocutrice officielle du Cégep auprès du COCD et assume notamment les responsabilités suivantes :

- Collaborer avec le COCD du ministère de l'Enseignement supérieur et avec la personne CSIO du Cégep à l'élaboration des divers éléments stratégiques et tactiques en sécurité de l'information en lien avec les préoccupations du ministère concernant les éléments suivants :
  - la politique et le Cadre de gestion de la sécurité de l'information;
  - la catégorisation des actifs et des mesures en sécurité appropriées;
  - les mesures de sécurité pour les actifs jugés critiques;
  - les processus formels en gestion des risques et des droits d'accès.
- Assister les responsables d'actifs informationnels du Collège pour ce qui est de la catégorisation de l'information relevant de leur responsabilité et de la réalisation des analyses de risques de sécurité de l'information.
- Collaborer avec le COCD au processus gouvernemental de gestion des incidents (registre) et au réseau d'alerte gouvernemental et proposer des réactions locales appropriées.
- Contribuer à l'auto-évaluation de la sécurité des systèmes informatiques et des réseaux informatiques du Cégep, notamment par des exercices d'audit de sécurité et des tests d'intrusion aux systèmes jugés à risque.

- Élaborer et maintenir à jour les guides ou directives portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunication en place au Cégep.
- Tenir à jour le registre des incidents reliés à la sécurité de l'information du Collège.
- Collaborer étroitement avec la personne CSIO et lui fournir le soutien technique nécessaire à l'exercice de ses responsabilités.

10.7 Direction des technologies de l'information (DTI)

En matière de sécurité de l'information, la DTI s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information. La DTI collabore étroitement avec la personne CSIO afin d'assurer une cohérence dans l'ensemble des mesures mises en place afin de sécuriser les actifs informationnels du Collège.

Plus particulièrement, la DTI doit :

- Appliquer et s'assurer du suivi des différentes mesures en sécurité de l'information prévues dans cette politique et dans le Cadre de gestion de la sécurité de l'information.
- Collaborer avec la ou le COMSI à la production, par le Collège, de la déclaration des risques et des incidents de sécurité de l'information à portée gouvernementale.
- Collaborer avec la Direction des ressources humaines à l'élaboration d'un programme de sensibilisation et de formation en matière de sécurité de l'information.
- Collaborer avec le Service des communications à l'élaboration d'un plan de communication lié à la sécurité de l'information.
- Collaborer à l'élaboration du Cadre de gestion de la sécurité de l'information et voir à son application, sa diffusion et sa mise à jour.
- 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.
- En collaboration avec la ou le CSIO, appliquer des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information. Notamment, lorsque les circonstances l'exigent, l'interruption ou la révocation temporaire des services d'un système d'information et ce, afin de préserver l'intégrité informationnelle du Cégep ou d'éviter la propagation de la menace.
- Participer aux enquêtes relatives à des contraventions à la présente politique autorisées préalablement par la Direction générale.
- Mettre en place un plan de continuité ou de relève des services en cas d'incident en sécurité de l'information ou accidentel (feu, dommage causé par l'eau, etc.) portant atteinte aux actifs informationnels.
- S'assurer des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

10.8 Service des ressources matérielles et du développement durable

Le service participe, avec la DTI et la personne CSIO, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep dont les salles des serveurs et les équipements sensibles (réseautique, télécommunication ou autres).

10.9 Direction des ressources humaines

En matière de sécurité de l'information, la Direction des ressources humaines doit obtenir de tout.e nouvel.le employé.e du Cégep, après lui en avoir montré la nécessité, son engagement au respect de la politique.

Organiser des activités de sensibilisation et des séances de formation aux employé.es du Cégep face à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en cette matière.

10.10 Service des communications

En collaboration avec la personne CSIO, le service est responsable de l'élaboration d'un plan de communication lié à la présente politique et du Cadre de gestion de la sécurité de l'information. Le service, en collaboration avec le comité de la sécurité de l'information (CSI), élaborera un plan de communication lors d'incidents en sécurité de l'information ayant un impact sur l'offre de services du Collège. En collaboration avec la DTI, il informe et sensibilise les membres de la communauté collégiale sur leurs responsabilités en ce qui a trait à la sécurité de l'information.

10.11 Responsables d'actifs informationnels

Le personnel d'encadrement est le détenteur d'actifs informationnels dans son champ de responsabilités. Dans les faits, il y a plusieurs responsables d'actifs informationnels dans un Cégep. La personne responsable d'actifs informationnels peut déléguer la totalité ou une partie de sa responsabilité à un.e autre membre du service.

La personne responsable d'actifs informationnels doit :

- Présenter la politique et le Cadre de gestion de la sécurité de l'information au personnel relevant de son autorité et aux tiers avec lesquels elle transige. Les sensibiliser envers leurs obligations en lien avec la Politique de sécurité de l'information et des dispositions du Cadre de gestion de la sécurité de l'information.
- Collaborer activement avec la ou le COMSI à la catégorisation de l'information du service sous sa responsabilité et à l'analyse des risques potentiels.
- 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 présente politique, du Cadre de gestion de la sécurité de l'information et des directives et procédures en cette matière.
- 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 tout consultant.e, fournisseur, partenaire, invité.e, organisme ou firme externe s'engage à respecter la politique et tout autre élément du Cadre de gestion de la sécurité de l'information.

- Rapporter à la DTI 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 personne CSIO ou ultimement à la Direction générale tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un.e membre du personnel à ce qui a trait à l'application de cette politique.
- Informer la DTI des accès aux différents systèmes ou logiciels des personnes utilisatrices sous sa responsabilité.

10.12 Responsable de la gestion documentaire

- 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 afin de se conformer aux bonnes pratiques en matière de sécurité de l'information.
- S'assurer de la conservation du patrimoine informationnel du Collège, de la préservation des preuves et du respect des lois.
- Collaborer étroitement avec les responsables d'actifs informationnels et la ou le COMSI, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

10.13 Responsable de l'accès à l'information et de la protection des renseignements personnels

La personne responsable de l'accès à l'information et de la protection des renseignements personnels 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) par le Collège. Elle s'assure du respect de la présente politique et du Cadre de gestion de la sécurité de l'information dans l'exercice de ses fonctions.

10.14 Utilisateurs

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

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

À cette fin, la personne utilisatrice doit :

- Se conformer à la présente politique et au Cadre de gestion de la sécurité de l'information et aux différentes procédures et directives en la matière.
- 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 (utilisateur employé).

- Respecter les mesures de sécurité mises en place, ne pas les contourner, ni modifier leur configuration, ni les désactiver.
- Signaler à la personne responsable des actifs informationnels de son service (utilisateur employé) 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.
- Informer la DTI de tout incident de sécurité de l'information (piratage ou intrusion d'un système informatique, vol d'identité, utilisation de virus informatique, etc.) dont elle a connaissance.

Le fournisseur externe qui, dans le cadre d'un mandat confié par le Collège, utilise ou accède aux actifs informationnels doit s'assurer que lui et ses employé.es respectent la politique et le Cadre de gestion de la sécurité de l'information.

11. SANCTIONS

- Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente politique et au Cadre de gestion de la sécurité de l'information, 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 des conventions collectives de travail en vigueur et du *Règlement sur les sanctions applicables, en cas d'infraction à certaines conditions de vie au Collège* (règlement #17).
- De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un.e invité.e, un.e consultant.e 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.
- La Direction générale décide de l'application de l'une ou l'autre, ou plusieurs de ces sanctions. Elle peut également transmettre à toute autorité judiciaire les informations colligées sur toute personne utilisatrice d'actifs informationnels ayant contrevenu à cette politique et qui portent à croire qu'une infraction à l'une ou l'autre, loi ou règlement en vigueur, a été commise. La personne contrevenante doit alors faire face à des mesures légales et s'expose à des poursuites judiciaires.

12. MISE À JOUR DE LA POLITIQUE

La personne chef de la sécurité de l'information organisationnelle (CSIO) assure la diffusion, la mise en œuvre et la mise à jour de la présente politique.

Afin d'assurer son adéquation aux besoins de sécurité du Cégep et s'ajuster aux nouvelles pratiques et technologies utilisées, la présente politique est révisée lors de tout changement important qui pourrait l'affecter.

Toute modification à la présente politique doit être sanctionnée par le conseil d'administration du Cégep sur recommandation de la Direction générale.

13. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil d’administration, soit le 20 septembre 2022 et remplacera la Politique relative à la sécurité de l’information et à l’utilisation des technologies de l’information (2015-CA01-07).

RÉFÉRENCES

La Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information s'inspire de :

- Fédération des cégeps, kit #2 projet Vigilance, 2019.
- Cégep de Beauce-Appalaches, Politique de sécurité de l'actif informationnel, décembre 2017.
- CSS de la Capitale, Politique sur la sécurité informatique, janvier 2021
- École de technologie supérieure, Politique de sécurité de l'information, 22 février 2007.
- Centre de service scolaire de la Capitale, Politique sur la sécurité de l'information, janvier 2021.
- Cégep Ahuntsic, Politique de sécurité de l'information, novembre 2018.
- Cégep de Maisonneuve, Politique de sécurité de l'information, juin 2019.
- Cégep de Sept-Îles, Politique de sécurité de l'information, octobre 2019.
- CSS région de Sherbrooke, Politique sur la sécurité informatique, 2020
- Université de Montréal, Politique sur la sécurité de l'information, version novembre 2020.
- Polytechnique Montréal, Politique de sécurité de l'information, septembre 2018.