

POLITIQUE DE LA SÉCURITÉ DE L'INFORMATION

SERVICE RESPONSABLE	Direction des technologies de l'information
ADOPTION	CA/455 – 1 ^{er} octobre 2025
MODIFICATIONS	



Table des matières

Préambule	3
1. Définitions	3
2. Champ d'application.....	5
3. Principes directeurs	6
4. Axes de gestion de la sécurité de l'information	7
5. Rôles et responsabilités.....	8
6. Sensibilisation et information à la communauté.....	11
7. Manquement aux règles de la politique.....	11
8. Date d'entrée en vigueur et révision.....	11

Préambule

Le cégep du Vieux Montréal reconnaît que l'information et les technologies qui la soutiennent sont essentielles à ses activités et à la réalisation de sa mission d'enseignement et de recherche. Compte tenu de leur valeur administrative, légale et financière, les actifs informationnels doivent être évalués de façon continue et protégés de manière appropriée tout au long de leur cycle de vie, conformément aux bonnes pratiques de sécurité de l'information et dans une approche de gestion des risques, quel que soit leur support ou leur emplacement.

Pour se conformer à ses obligations réglementaires et légales, le cégep du Vieux Montréal doit adopter, maintenir à jour et veiller à l'application d'une politique de sécurité de l'information afin d'assurer la mise en place de processus formels en matière de sécurité informationnelle pour encadrer la gestion des risques, incluant ceux de l'intelligence artificielle (IA), la gestion des accès aux actifs informationnels, la gestion des incidents et la gestion de la continuité des activités.

1. Définitions

1.1. Actif informationnel

Tout document définit au sens de l'article 3 de la *Loi concernant le cadre juridique des technologies de l'information*. Cette loi définit le document comme étant « un ensemble constitué d'information portée par un média. L'information y est délimitée et structurée, de façon tangible ou logique selon le média qui la porte, et 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 transcritibles sous l'une de ces formes ou en un autre système de symboles. [...] est assimilée 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. »

1.2. Code d'accès

Mécanisme d'identification et d'authentification par un code individuel et un mot de passe ou de ce qui en tient lieu, notamment une carte magnétique ou une carte à puce, servant à identifier de façon unique une utilisatrice ou un utilisateur qui utilise un actif informationnel du Cégep.

1.3. Confidentialité

La propriété d'une information d'être accessible uniquement aux personnes ou aux entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

1.4. Cycle de vie de l'information

L'ensemble des étapes que franchit l'information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation du Cégep.

1.5. Détentrice ou détenteur

Une personne responsable détenant l'autorité au sein d'un service qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels du Cégep.

1.6. Disponibilité

La propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

1.7. Équipement informatique

Les postes de travail informatisés, leurs accessoires périphériques de lecture, d'emmagasiner, de reproduction, d'impression, de communication, de réception et de traitement de l'information et tout équipement de télécommunications et de réseautique.

1.8. Information

Un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

1.9. Intégrité

La propriété d'une information de ne subir aucune altération ni destruction sans autorisation ou de façon erronée, laquelle information est conservée sur un support et préservée avec des moyens lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

1.10. Sécurité de l'information ou sécurité informationnelle

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

1.11. Technologies de l'information

Regroupent les équipements techniques, principalement de l'informatique, de l'audiovisuel, du multimédia, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie) qui permettent aux utilisatrices et utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre de l'information

1.12. Personne utilisatrice

Toute personne qui, à titre d'employée ou d'employé, de consultante ou de consultant, de partenaire, de bénévole, de stagiaire, de fournisseur, d'étudiante ou d'étudiant, de gestionnaire ou de public, utilise les actifs informationnels du Cégep et qui accède par le truchement des réseaux numériques et non numériques à de l'information que le Cégep détient dans l'accomplissement de sa mission. Les membres du personnel ainsi que les étudiantes et étudiants sont les premières personnes utilisatrices de l'information du Cégep.

2. Champ d'application

2.1. Personne utilisatrice

Personnes visées

Cette politique s'applique sans exception à l'ensemble des personnes utilisatrices, peu importe leur statut, appelées à utiliser les actifs informationnels du Cégep.

2.2. Actifs visés

Cette politique vise toutes les informations et les actifs informationnels appartenant au Cégep, ou détenus par un tiers, mais appartenant au Cégep, utilisés et détenus par un tiers au bénéfice ou au nom du Cégep, et ce, quel que soit le média de conservation (électronique, technologique, papier, etc.).

Cette politique vise également tous les systèmes informatiques, sur site ou hébergés incluant les environnements infonuagiques, qui traitent les données, y compris tout le matériel informatique ou tout objet connecté qui interagit avec les services informatiques du Cégep. La sécurité de l'information liée de l'intelligence artificielle est aussi couverte par cette politique afin d'encadrer la gestion des risques et la gestion des accès aux actifs informationnels dans le but d'assurer la confidentialité et l'intégrité de l'information institutionnelle.

2.3. Activités visées

Cette politique concerne l'ensemble des activités conduites dans le périmètre de ses locaux ou à distance, entrant dans le cycle de vie de l'information, à savoir, la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation et la destruction des actifs informationnels du Cégep.

2.4. Fondements juridiques et conformité

Cette politique repose sur divers fondements juridiques, notamment la *Directive gouvernementale sur la sécurité de l'information* (2021) et le *Cadre gouvernemental de gestion de la sécurité de l'information* (2021). Elle se conforme aux lois et aux règlements applicables, en particulier les suivants :

- a) *La Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1) ;
- b) *La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1) ;
- c) *La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25) ;
- d) *La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03) ;
- e) *Le Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles* (LRQ, chapitre G-1.03, r. 1).

3. Principes directeurs

Le cégep du Vieux Montréal doit assurer la sécurité des ressources informationnelles et de l'information qu'il utilise ou détient, et ce, tout au long de son cycle de vie.

3.1. Protection de l'information

Dans le respect des bonnes pratiques, la sécurité de l'information s'articule autour des trois principes suivants :

a) **Disponibilité**

La disponibilité garantit que les utilisatrices et utilisateurs autorisés d'un système ont un accès opportun aux informations contenues dans ce système ainsi qu'au réseau. Les informations doivent être accessibles en temps utile et de la manière requise par une utilisatrice ou un utilisateur autorisé. Afin d'assurer cette disponibilité, des mesures de contrôles doivent être mises en place.

b) **Intégrité**

L'intégrité des données consiste à garantir que les données n'ont pas été modifiées au cours de leur communication, qu'il s'agisse de données au repos, en transit ou en mémoire. Afin d'assurer l'intégrité des données, des mesures de sécurité physiques et d'accès logiques doivent être mises en place.

c) **Confidentialité**

La confidentialité vise à empêcher tout accès non autorisé à des informations sensibles. Elle a pour but de s'assurer qu'une information ou une donnée soit accessible uniquement par les personnes autorisées. La confidentialité de l'information doit aussi être assurée tout au long de son cycle de vie. Afin de garantir la confidentialité, des mesures de contrôle doivent être mises en place.

3.2. Classification des données numériques

L'information constitue une ressource essentielle qui doit être protégée tout au long de son cycle de vie. Pour cette raison, il est primordial de garder à jour l'inventaire de l'ensemble des actifs informationnels de l'organisation. L'un des premiers intrants de la sécurité de l'information est la connaissance de la sensibilité de l'information des actifs informationnels d'une organisation.

La classification des données est un processus qui permet d'évaluer le degré de sensibilité des actifs dans le but d'en déterminer le niveau de protection. La classification est une responsabilité partagée entre la Direction des technologies de l'information (DTI), la personne responsable de la protection des renseignements personnels ainsi que la détentrice ou le détenteur de l'information.

Il est essentiel de réévaluer périodiquement la classification des données afin de garantir qu'elle reste appropriée. Cette réévaluation doit tenir compte des changements dans les obligations légales et contractuelles, les technologies, les environnements physiques et les conditions environnementales, ainsi que des évolutions dans l'utilisation et la valeur des données pour l'établissement. Il est également important de considérer l'évolution des risques et des menaces.

4. Axes de gestion de la sécurité de l'information

La *Politique de sécurité de l'information* du Cégep se base sur cinq axes fondamentaux de gestion.

4.1. Gestion des identités et des accès

La gestion des identités et des accès est encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de toute information détenue par le Cégep soient strictement réservés aux personnes autorisées afin de protéger la confidentialité.

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

4.2. Gestion des vulnérabilités

La gestion des vulnérabilités se caractérise par un déploiement de mesures pour maintenir à jour les logiciels du parc informatique afin de garder les vulnérabilités au niveau le plus bas possible et de mitiger les probabilités d'une cyberattaque. Une veille et une gestion de notification des vulnérabilités venant des fournisseurs ou des prestataires de services doivent être en place pour qu'elles soient évaluées et corrigées, le cas échéant.

4.3. Gestion du risque

La gestion des risques touchant l'actif informationnel du Cégep est basée sur une analyse des menaces encourues reliées à l'intégrité, la disponibilité et la confidentialité de l'information détenue par le Cégep.

De cette analyse découlent des directives reliées à l'utilisation et l'opération des systèmes d'information ainsi qu'aux résultats escomptés.

4.4. Gestion des incidents

La gestion des incidents se caractérise par la procédure de compte rendu, d'analyse relativement aux incidents de sécurité de l'information et de mesures correctives pour y donner suite. Le Cégep a mis en place une procédure de compte rendu lorsque survient un incident impliquant la sécurité de l'information.

Des mesures correctives seront apportées à la suite d'une analyse des incidents de sécurité de l'information. Les mesures déployées visent à assurer la continuité des services. Dans la gestion des incidents, le Cégep peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'actif informationnel.

4.5. Gestion de la reprise et de la continuité des affaires

La gestion de la reprise et de la continuité des affaires se caractérise par la mise en place des processus pour identifier les incidents opérationnels majeurs susceptibles de menacer l'organisation tels les catastrophes naturelles, les pannes d'électricité, de télécommunication et informatiques, le piratage, le terrorisme, les pandémies, etc. L'identification de ces incidents permet d'évaluer leurs impacts sur les activités de l'organisation et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

5. Rôles et responsabilités

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des responsabilités à tous les niveaux de l'organisation et la mise en place de processus de gestion de la sécurité de l'information permettant une reddition de comptes adéquate.

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.

5.1. Cheffe ou chef de la sécurité de l'information organisationnelle (CSIO)

La personne à la Direction des technologies de l'information occupe la fonction de CSIO et assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein du Cégep.

La ou le CSIO est responsable de la diffusion, de la mise en application, de l'évaluation et de la révision de la politique. Il effectue et participe aux analyses de risques en sécurité de l'information, gère le processus de gestion, de déclaration des incidents et de résolution de problème et contribue à sa mise en place. Il contribue également au processus de gestion des droits d'accès à l'information.

La ou le CSIO est aussi responsable de la prise en charge des exigences de la 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 ou le CSIO désigne la coordonnatrice ou le coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) et voit à ce que le personnel de la DTI l'appuie dans l'identification des mesures de sécurité permettant de protéger adéquatement les actifs informationnels du Cégep afin d'intégrer des mesures de protection en fonction du niveau de sensibilité de l'information, en tenant compte des exigences réglementaires, d'affaires, légales ou contractuelles.

La ou le CSIO est responsable de voir à la mise en place d'activités de sensibilisation, de formation et d'information conformément à l'article 6.

5.2. Coordonnatrice ou coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

La personne assumant la fonction de COMSI agit sur le plan opérationnel.

Elle intervient dans la mise en œuvre des mesures et apporte le soutien nécessaire à la ou au CSIO de l'établissement, notamment en matière de gestion des incidents et des risques en sécurité de l'information, ainsi que dans la mise en œuvre des mécanismes de la catégorisation des actifs informationnels.

La ou le COMSI représente le Collège auprès du réseau d'alerte gouvernemental.

Cette personne est responsable de l'application du processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) pour le Collège, en soutien à la ou au CSIO.

Il collabore avec la ou le CSIO du Cégep à l'élaboration des divers éléments stratégiques et tactiques en sécurité informationnelle, notamment, le maintien d'un registre des événements et des incidents liés à la sécurité de l'information.

5.3. Responsable de la protection des renseignements personnels

La personne gestionnaire à la Direction des communications et des affaires corporatives, responsable de la protection des renseignements personnels, veille à assurer le respect et la mise en œuvre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

5.4. Direction des ressources humaines (DRH)

En matière de sécurité de l'information, la Direction des ressources humaines (DRH) s'assure, en collaboration avec la DTI, que les responsabilités des intervenantes et intervenants concernant la sécurité de l'information et le respect de la présente politique sont inscrites dans les descriptions de tâches des membres du personnel de la DTI. La Direction des ressources humaines doit également

obtenir de toute nouvelle personne employée au Cégep son engagement au respect de la présente politique.

5.5. Détentrice ou détenteur responsable d'actifs informationnels

Tout gestionnaire est responsable des actifs informationnels de son service. Cette personne a pour mission de veiller à l'accessibilité, à l'utilisation appropriée et à la sécurité des actifs informationnels relevant de ce service, et ce, en étroite collaboration avec la DTI. À ce titre, la personne cadre :

- a) Participe à la classification des données numériques de l'unité sous sa responsabilité et à l'analyse de risques, en collaboration avec la DTI et la personne responsable de la protection des renseignements personnels
- b) Veille à la protection de l'information et des systèmes d'information sous sa responsabilité, en collaboration avec la DTI
- c) Rapporte aux COMSI tout événement, menace ou incident porté à sa connaissance liée à la sécurité de l'information
- d) Collabore avec la DTI à la mise en œuvre de toute mesure pour améliorer la sécurité de l'information afin de remédier à un incident au besoin.

5.6. Personne utilisatrice

Toute personne utilisatrice a l'obligation de protéger les actifs informationnels mis à sa disposition par le Cégep. Une personne 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. Elle doit se conformer aux politiques et aux directives en vigueur dans le cadre de ses activités professionnelles ou d'études lorsqu'elle y partage des actifs informationnels ou utilise des dispositifs de technologies de l'information ou des systèmes d'information.

À cette fin, la personne utilisatrice doit :

- a) 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
- b) Être responsable des actions résultant de l'usage de son identifiant, de son code d'accès ou de son mot de passe
- c) Signaler immédiatement à son supérieur tout acte dont il a connaissance susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du Cégep
- d) Au besoin, participer à la classification des données de son service
- e) 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 approprié à son utilisation et aux fins auxquelles ils sont destinés dans l'exercice de ses fonctions

- f) Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver
- g) Se conformer aux exigences légales portant sur l'utilisation des actifs informationnels à l'égard desquels des droits de propriété intellectuelle pourraient exister
- h) 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
- i) Participer aux activités de sensibilisation et de formation en cybersécurité
- j) Au moment de son départ du Cégep, remettre 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.

6. Sensibilisation et information à la communauté

La sécurité de l'information repose notamment sur l'adoption de comportements sécuritaires et sur la responsabilisation individuelle.

La Direction des technologies de l'information maintiendra un programme continu de sensibilisation à la sécurité de l'information destiné à l'ensemble des utilisatrices et utilisateurs incluant des campagnes de simulation d'hameçonnage. À cet égard, les membres de la communauté du Cégep doivent être sensibilisés :

- a) À la sécurité de l'information et des systèmes d'information du Cégep
- b) Aux conséquences d'une atteinte à la sécurité
- c) À leurs rôles et à leurs responsabilités en la matière.

7. Manquement aux règles de la politique

Toute personne qui contrevient à la présente politique engage sa responsabilité. Il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information ne soit pas protégée adéquatement et s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention en vertu de la loi, des règles internes ou de tout autre encadrement applicable. De même, toute contravention à la politique, qu'elle soit perpétrée par un tiers, notamment un fournisseur, un partenaire, une invitée ou un invité, une consultante ou un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au Cégep, ainsi que des dispositions de la législation applicable.

8. Date d'entrée en vigueur et révision

La politique entre en vigueur à la date de son adoption par le conseil d'administration. Elle pourra faire l'objet d'une révision en fonction de l'évolution des obligations législatives et réglementaires afin de tenir compte des nouvelles orientations gouvernementales ou de l'évolution des pratiques en sécurité de l'information.