CÉGEP DE LANAUDIÈRE

Titre : **Politique de sécurité de l'information**

Adoption par le conseil d'administration :

Résolution : **CARL-130924-11**

Date : **24 septembre 2013**

Révisions :

Résolution : **CARL-230614-13**

Date : **14 juin 2023**

Résolution : **CARL-240618-07**

Date : **18 juin 2024**

TABLE DES MATIÈRES

PRÉAMBULE

Le Cégep régional de Lanaudière, ci-après appelé « le Cégep », reconnaît que l'information et les technologies qui la supportent sont essentielles à ses opérations courantes et à l'accomplissement de sa mission d'enseignement et de recherche, et vu la valeur administrative, légale et financière de ses actifs informationnels, ils doivent faire l'objet d'une évaluation continue, d'une utilisation et d'une protection appropriées et adéquates tout au long de leur cycle de vie, selon les bonnes pratiques en matière de sécurité informationnelle et avec une approche de gestion des risques, quel qu'en soit le support ou l'emplacement.

L'application de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre. G-1.03), de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25), et de la *Directive gouvernementale sur la sécurité de l'information* (2021) du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics, impose des obligations importantes aux établissements collégiaux.

Pour se conformer et répondre à ses obligations réglementaires et légales, le Cégep régional de Lanaudière doit adopter, garder à jour et veiller à l'application d'une politique de sécurité de l'information (SI) pour assurer la mise en place des processus formels de la sécurité de l'information afin d'encadrer la gestion des risques, la gestion des accès aux actifs informationnels, la gestion des incidents et la gestion de la continuité des activités.

1. OBJECTIF DE LA POLITIQUE

La présente politique constitue le cadre général qui vise la gestion des actifs informationnels dans le respect des droits et obligations du Cégep en cette matière pour garantir et répondre aux objectifs de sécurité de l'information et plus spécifiquement pour :

- Assurer la protection de l'actif informationnel tout au long de son cycle de vie, quel que soit le support ou l'emplacement ;
- Assurer la disponibilité de l'information pour qu'elle soit accessible au moment voulu et utilisable à la demande par l'entité autorisée ;
- Assurer l'intégrité de l'information en la préservant contre toute destruction, modification et altération de quelque façon sans autorisation ;
- Préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou divulguée à des personnes, entités ou processus non autorisés ;
- Assurer le respect de la vie privée des individus, notamment la protection des renseignements personnels (PRP) ;
- Regrouper les lignes directrices et les rôles et responsabilités des intervenants en sécurité ;
- Identifier et classifier les actifs informationnels du Cégep selon leurs degrés de criticités et veiller constamment à leur évaluation ainsi que leur protection adéquate ;
- Assurer la conformité aux lois et cadres réglementaires ;
- Mettre en place un plan de continuité des activités et de relève informatique.

2. CADRE LÉGAL ET NORMATIF

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales. Pour plus de précisions, voir l'**Annexe 1**.

3. CHAMP D'APPLICATION DE LA POLITIQUE

Personnes visées

Cette politique vise, sans exception, l'ensemble des personnes physiques et morales, régulières ou occasionnelles, peu importe son statut, appelées à utiliser les actifs informationnels du Cégep citant entre autres :

- Le personnel à l'emploi du Cégep ;
- Les étudiantes et étudiants du Cégep ;
- Les partenaires, fournisseurs, contractants et tiers du Cégep.

Actifs visés

La politique vise aussi toutes les informations et les actifs informationnels :

- Appartenant au Cégep ;
- 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 support de conservation (électronique, technologique, papier, etc.).

Activités visées

Cette politique concerne l'ensemble des activités 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, qu'elles soient menées dans le périmètre de ses locaux, dans un autre endroit ou à distance.

4. RÔLES ET 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.

4.1. Conseil d'administration

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

4.2. La direction générale

La direction générale est le premier responsable de la sécurité de l'information. Elle assume le processus de délégation des rôles de CSIO et COMSI.

4.3. Chef de la sécurité de l'information organisationnelle (CSIO)

La personne assumant la fonction de CSIO est un membre du personnel d'encadrement d'un organisme public. Ce chef assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. Le CSIO est nommé par le conseil d'administration et la fonction de CSIO est déléguée par la direction générale.

Le CSIO est responsable de la diffusion et de la mise en application de la politique.

4.4. Comité de sécurité de l'information

Sous la responsabilité du chef de la sécurité de l'information organisationnelle (CSIO), le comité de sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information, au niveau stratégique, au sein du Cégep. Ce comité est notamment chargé de formuler des recommandations.

4.5. Comité régional de planification et de coordination (CRPC)

Le comité régional de planification et de coordination met en œuvre les orientations stratégiques. Il peut également approuver des directives et des procédures afin de préciser ou de soutenir l'application de la présente politique.

4.6. Responsable de la protection des renseignements personnels (PRP)

Le responsable de la PRP veille à assurer le respect et la mise en œuvre de la loi sur la protection des renseignements personnels afin de mettre en œuvre des politiques et pratiques encadrant la gouvernance des renseignements personnels.

4.7. Direction des technologies de l'information (DTI)

La direction des technologies de l'information assume la responsabilité de l'application de la présente politique. Elle s'assure 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 DTI élabore et met en place le programme de sensibilisation et de formation du personnel du Cégep en matière de sécurité de l'information.

De plus, elle participe, avec le CSIO, à l'identification des mesures de sécurité physique 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.

4.8. 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 au CSIO de l'établissement, notamment en matière de gestion des incidents et des risques en sécurité de l'information.

Le COMSI représente l'organisme public auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) dans son cégep, en soutien à son chef de la sécurité de l'information organisationnelle (CSIO).

Il collabore auprès du CSIO du Cégep à l'élaboration des divers éléments stratégiques et tactiques en sécurité informationnelle :

- 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 ;
- Contribue au processus formel de gestion des droits d'accès à l'information.

4.9. Direction des ressources humaines

En matière de sécurité de l'information, la direction des ressources humaines doit :

- Vérifier les antécédents des candidats à l'embauche et des membres du personnel impliqués dans la sécurité de l'information ;

- S’assurer que les responsabilités des intervenants concernant la sécurité de l’information et le respect de la présente politique, ainsi que du cadre normatif des ressources informationnelles, sont inscrites dans les descriptions de tâches des membres du personnel ;
- Informer et obtenir de tout nouvel employé du Cégep son engagement au respect de la présente politique ;
- Accompagner et appuyer les gestionnaires dans la gestion des sanctions appropriées lors de violation des politiques, règlements, directives et code de conduite touchant à la sécurité de l’information.

4.10. Responsable d’actifs informationnels (détenteur)

La personne assumant le rôle de responsable d’actifs informationnels est la personne-cadre détenant l’autorité au sein d’un service, qu’elle soit d’ordre pédagogique ou d’ordre administratif. Son rôle consiste à veiller à l’accessibilité, à l’utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Le responsable :

- Participe à la catégorisation de l’information de l’unité sous sa responsabilité et à l’analyse de risques ;
- Veille à la protection de l’information et des systèmes d’information en conformité avec la *Politique de sécurité de l’information* (SI) ;
- Rapporte tout événement ou toute menace liée à la SI ;
- Collabore à la mise en œuvre de toute mesure pour améliorer la SI afin de remédier à un incident au besoin.

4.11. Utilisateurs

La responsabilité de la sécurité de l’information du Cégep incombe à tous les utilisateurs des actifs informationnels du Cégep. Tout utilisateur qui accède à une information, qui la consulte ou qui la traite, est responsable de l’utilisation qu’il en fait et doit procéder de manière à protéger cette information.

À cette fin, l’utilisateur doit :

- 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 ;
- Être responsable des actions résultant de l’usage de son identifiant, de son code d’accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers, à moins qu’il démontre que les actions posées par un tiers ne découlent pas d’une négligence ou d’une malveillance de sa part ;
- Signaler au responsable d’actifs informationnels (détenteur) de son unité tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l’information du Cégep ;
- 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 approprié à son utilisation et aux fins auxquelles ils sont destinés ;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver ;
- 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.

5. PRINCIPES DIRECTEURS

Le Cégep s'engage fermement à appliquer les meilleures pratiques en matière de sécurité de l'information. Dans cette optique, il veille à une parfaite connaissance des données à protéger et à l'identification précise des responsabilités afférentes. Cette démarche inclut une évaluation minutieuse des risques ainsi que des menaces susceptibles de compromettre la disponibilité, l'intégrité et la confidentialité des informations. Sur cette base, des mesures de sécurité adaptées et cohérentes sont déployées pour atténuer les risques identifiés. Une attention particulière est portée à la protection des renseignements personnels et de toute information confidentielle.

Le Cégep s'engage également à promouvoir de façon continue les meilleures pratiques en matière de protection des actifs informationnels. À cet effet, il développe et diffuse régulièrement des programmes de sensibilisation et de formation destinés à tous les utilisateurs, visant à renforcer leur compréhension des enjeux liés à la sécurité de l'information et à les habiliter à adopter des comportements responsables.

6. AXES DE GESTION FONDAMENTAUX

Pour garantir l'efficacité des mesures de sécurité de l'information, il est impératif de définir clairement les rôles et responsabilités de chaque intervenant au sein du Cégep. Cela passe par la mise en place d'un cadre de gestion de la sécurité qui favorise une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information sont réévaluées périodiquement 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 cinq axes fondamentaux de gestion.

6.1. Gestion des identités et des accès (GIA)

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.

6.2. Gestion des vulnérabilités

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

6.3. Gestion du risque

La gestion des risques touchant l'actif informationnel du Cégep est basée sur une analyse des menaces encourues reliées à la disponibilité, à l'intégrité et la confidentialité (DIC) 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.

Une catégorisation à jour soutient l'analyse de risques en permettant de connaître la valeur (DIC) de l'information à protéger.

6.4. Gestion des incidents

La gestion des incidents implique la mise en œuvre de mécanismes de rapports et d'analyse d'incidents de sécurité, ainsi que de mesures correctives pour y remédier. L'objectif principal de ces mesures est d'assurer la continuité des services.

Dans le cadre de la gestion des incidents, le Cégep est habilité à exercer ses pouvoirs et ses prérogatives en réponse à toute utilisation inappropriée de ses actifs informationnels.

Le Cégep met en place des mesures de sécurité de l'information afin de garantir la continuité de ses services. À cette fin, il s'engage à :

- Prévenir l'occurrence d'incidents liés à la sécurité de l'information en mettant en place des mesures préventives adéquates.
- Gérer efficacement ces incidents pour en atténuer les conséquences et rétablir les activités ou les opérations dans les meilleurs délais.

6.5. 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 ou de télécommunication, les pannes 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.

7. SENSIBILISATION ET FORMATION

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

À cet égard, les membres de la communauté du Cégep doivent être sensibilisés :

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

Les organisations s'engagent sur une base régulière à sensibiliser et à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à la sécurité de ces actifs ainsi qu'à leur rôle et leurs obligations en la matière. L'utilisateur a la responsabilité de participer à ces activités de sensibilisation et de formation. Par ailleurs, les organisations favorisent le recours aux services communs de formation en sécurité de l'information.

8. SANCTIONS

En cas de contravention à la présente politique, 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 ne soit pas protégée adéquatement.

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l'information qui en découlent, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles administratives ou disciplinaires internes applicables.

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

9. MISE À JOUR DE LA POLITIQUE

La présente politique sera révisée lorsque nécessaire en fonctions des modifications aux lois, règlements ou directives applicables, et ce, régulièrement.

10. ENTRÉE EN VIGUEUR

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

ANNEXE 1

Fondements légaux :

- La Directive gouvernementale sur la sécurité de l'information ;
- Cadre gouvernemental de gestion de la sécurité de l'information ;
- Dispositions légales et administratives en sécurité de l'information ;
- Aide-mémoire : Politique gouvernementale en cybersécurité ;
- La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1) ;
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1) ;
- La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, 2021, chapitre 25) ;
- Règlement sur les incidents de confidentialité ;
- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03) ;
- 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 ;
- Règles relatives à la gestion des projets en ressources informationnelles ;
- Règles relatives à la planification et à la gestion des ressources informationnelles ;
- La Loi sur les archives (LRQ, chapitre A-21.1) ;
- Les lois sectorielles régissant la mission de chaque organisme ;
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics ;
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2) ;
- La Charte des droits et libertés de la personne (LRQ, chapitre C-12) ;
- Le Code civil du Québec (LQ, 1991, chapitre 64) ;
- Le Code criminel (LRC, 1985, chapitre C-46) ;
- Loi sur la fonction publique (RLRQ, chapitre F-3.1.1) ;
- Toute autre loi ou règle applicable.

Fondements normatifs :

- Le cadre de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale ;
- Le cadre gouvernemental de gestion de la sécurité de l'information ;
- Les normes internationales, notamment ISO 27000 et NIST 800-60 ;
- Les pratiques gouvernementales en matière de sécurité de l'information.

GLOSSAIRE

Actif informationnel : information numérique, document numérique, système d'information, documentation, équipement informatique, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitué par le Cégep pour mener à bien sa mission.

Autorisation : attribution par une autorité de droits d'accès aux actifs informationnels qui consiste en un privilège d'accès accordé à une personne, à un dispositif ou à une entité.

Cadre de gestion : l'ensemble de consignes que sont les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues qui encadrent les activités d'un établissement tel qu'un cégep.

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

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 carte à puce, servant à identifier de façon unique un utilisateur qui utilise un actif informationnel du Cégep.

Confidentialité : propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées.

Cycle de vie de l'information : l'ensemble des étapes que parcourt 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.

Détenteur : une personne qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels du Cégep.

Disponibilité : propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

Équipement informatique : ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communication, de réception et de traitement de l'information, et tout équipement de télécommunication.

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.

Incident de sécurité de l'information à portée gouvernementale : la conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale, nécessitant une intervention concertée au plan gouvernemental.

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

Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

Renseignement personnel : une information concernant une personne physique et qui permet de l'identifier.

Responsable d'actifs informationnels : le membre du personnel cadre détenant la plus haute autorité au sein d'une unité académique 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. Aux fins de l'application de la présente politique, il peut s'agir d'un autre membre du personnel cadre de l'unité désigné par la personne qui détient la plus haute autorité au sein de l'unité.

Sécurité de l'information : la protection de l'information et des systèmes d'information contre les risques et les incidents.

Système d'information : l'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

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