Cégep de la Gaspésie et des Îles

Politique de sécurité de l'information

Document préparé par
la Direction des ressources informationnelles

Approuvé par le conseil d'administration le 2023-06-28

Table des matières

PRÉAMBULE

Le Cégep de la Gaspésie et des Îles reconnaît que l'information et les technologies qui la soutiennent sont essentielles à ses activités courantes et à l'accomplissement de sa mission d'enseignement et de recherche. En raison de leur valeur administrative, légale et financière, les actifs informationnels doivent faire l'objet d'une évaluation continue. Le Cégep doit les utiliser et les protéger de manière appropriée tout au long de leur cycle de vie, et ce, en respectant les bonnes pratiques en matière de sécurité informationnelle et en appliquant une approche de gestion des risques, indépendamment du support ou de l'emplacement de ces actifs.

Des obligations importantes sont imposées aux établissements collégiaux par l'entremise 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.

Pour se conformer à ses obligations réglementaires et légales, le Cégep de la Gaspésie et des Îles doit adopter une politique de sécurité de l'information, la maintenir à jour et veiller à son application. Il doit assurer la mise en place de processus formels relatifs à 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.

CADRE LÉGAL ET NORMATIF

Le présent document prend appui sur des fondements légaux et normatifs tels que des lois, des directives, des normes, des standards et des pratiques gouvernementales.

La présente politique est soumise, notamment, aux dispositions suivantes :

- La *Directive gouvernementale sur la sécurité de l'information*;
- Le cadre gouvernemental de gestion de la sécurité de l'information;
- 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);
- Le *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);
- 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*;
- Les règles relatives à la gestion des projets en ressources informationnelles;
- Les 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);
- Le cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;

- 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.

De plus, elle complète les politiques suivantes du Cégep :

- La Politique de gestion intégrée des documents;
- La Politique sur la confidentialité.

DÉFINITIONS

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

Code d'accès : mécanisme d'identification et d'authentification par l'entremise d'un code individuel et d'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 personne qui utilise un actif informationnel du Cégep.

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

Cycle de vie de l'information : ensemble des étapes que parcourt une information, de sa création jusqu'à sa conservation ou sa destruction en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, en conformité avec le calendrier de conservation 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 télécommunications.

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

Plan de relève informatique : ensemble de procédures qui décrivent de façon précise les mesures à suivre pour remettre en état de fonctionnement un système informatique à la suite d'une panne ou d'un sinistre majeur.

Risques liés à la sécurité de l'information : tout événement qui survient lors du traitement, de l'utilisation ou de l'entreposage de l'information, comportant un degré d'incertitude et qui pourrait porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information et causer un préjudice.

Technologies de l'information : ensemble des 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 ainsi que de stocker, de manipuler, de produire et de transmettre de l'information.

CHAMP D'APPLICATION DE LA POLITIQUE

Cette politique s'adresse, sans exception, à l'ensemble des personnes physiques et morales, permanentes ou occasionnelles, peu importe leur statut, appelées à utiliser les actifs informationnels du Cégep, incluant 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 tous 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 de l'actif (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 conduites dans le périmètre de ses locaux, dans un autre endroit ou à distance.

OBJECTIF DE LA POLITIQUE

La présente politique constitue le cadre général qui vise la gestion des actifs informationnels dans le respect des droits et des obligations du Cégep en cette matière pour 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 de l'entité autorisée;
- Assurer l'intégrité de l'information en la préservant contre toute destruction, toute modification et toute altération réalisées de quelque façon sans autorisation;
- Préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou de ne pas la divulguer à des personnes, à des entités ou à des processus non autorisés;
- Regrouper les lignes directrices et les rôles et responsabilités des personnes intervenant en sécurité;
- Recenser et classifier les actifs informationnels du Cégep selon leur degré de criticité et veiller constamment à leur évaluation ainsi qu'à leur protection adéquate;
- Assurer la conformité aux lois et aux cadres réglementaires;
- Mettre en place un plan de continuité des activités et de relève informatique;
- Assurer le respect de la vie privée des personnes, notamment la confidentialité des renseignements personnels.

PRINCIPES DIRECTEURS

Protection de l'information[1]

La sécurité de l'information s'articule autour des trois principes suivants :

- Disponibilité

La disponibilité garantit que les utilisatrices et utilisateurs autorisés d'un système ont un accès opportun et ininterrompu 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 personne autorisée. Afin d'aider à assurer cette disponibilité, des mesures de contrôle doivent être mises en place.

- Intégrité

L'intégrité des données consiste à garantir que les données n'ont pas été modifiées d'aucune façon 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.

- 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 est accessible uniquement aux personnes autorisées. La confidentialité doit aussi être assurée tout au long du cycle de vie de l'information. Afin de garantir la confidentialité, des mesures de contrôle doivent être mises en place.

Catégorisation de l'information

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 maintenir 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 catégorisation des actifs informationnels en matière de sécurité de l'information est un processus

[1] Publication NIST SP800-53

qui permet d'évaluer le degré de sensibilité des actifs dans le but de déterminer leur niveau de protection.

Il est important de réévaluer périodiquement la catégorisation des actifs informationnels pour s'assurer que la catégorisation attribuée est toujours appropriée en fonction des modifications des obligations légales et contractuelles ainsi que des changements relatifs à l'utilisation des données ou à leur valeur pour l'établissement. Cette évaluation devrait être effectuée par la personne qui détient l'actif.

RÔLES ET RESPONSABILITÉS

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

Direction générale

La Direction générale assume le processus de délégation des rôles de cheffe ou chef de la sécurité de l'information organisationnelle (CSIO) et de coordonnatrice ou coordonnateur organisationnel des mesures de sécurité de l'information (COMSI). À la demande du conseil d'administration, la Direction générale l'informe des orientations stratégiques, de l'évaluation de risques, des plans d'action, des bilans de sécurité et des redditions de comptes en matière de sécurité de l'information.

Responsable de la protection des renseignements personnels

La personne responsable de la protection des renseignements personnels assure le respect et la mise en œuvre de la *Loi sur la protection des renseignements personnels* et de l'ensemble des politiques et des pratiques encadrant la gouvernance des renseignements personnels.

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

La personne assumant la fonction de CSIO est membre du personnel d'encadrement de la Direction des ressources informationnelles du Cégep. Elle assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation.

La fonction de CSIO est déléguée par la Direction générale. La personne qui occupe cette fonction a le mandat de présenter annuellement à la Direction générale les orientations stratégiques, les

évaluations de risques, les plans d'action, les bilans de sécurité ainsi que les redditions de comptes en matière de sécurité de l'information.

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 personne occupant les fonctions de CSIO au sein de l'établissement, notamment en matière de gestion des incidents et des risques en sécurité de l'information.

La ou le COMSI représente l'organisme public 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) au Cégep, en soutien à la personne assumant la fonction de CSIO.

La ou le COMSI collabore avec la ou du CSIO du Cégep pour élaborer divers éléments stratégiques et tactiques en sécurité informationnelle. Cette personne doit :

- Maintenir à jour le registre des événements et des incidents liés à la sécurité de l'information;
- Effectuer des analyses de risques en sécurité de l'information;
- Gérer le processus de gestion, de déclaration des incidents et de résolution de problèmes et contribuer à sa mise en place;
- Contribuer au processus formel de gestion des droits d'accès à l'information.

Direction des ressources informationnelles (DRI)

La Direction des ressources informationnelles s'assure de la prise en charge des exigences de la sécurité de l'information dans l'exploitation des systèmes de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information.

De plus, elle participe, avec la ou le CSIO, à la définition des mesures de sécurité physique qui permettent de protéger adéquatement les actifs informationnels du Cégep en fonction du niveau de sensibilité de l'information et des exigences réglementaires, d'affaires, légales ou contractuelles.

Direction des ressources humaines

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

- Vérifier les antécédents des candidates et des candidats à l'embauche ainsi que des membres du personnel impliqués dans la sécurité de l'information, selon leur fonction occupée dans l'organisation et les accès qui leur sont accordés;
- S'assurer que les descriptions de tâches des membres du personnel incluent les responsabilités relatives à la sécurité de l'information, au respect de la présente politique et au respect du cadre normatif des ressources informationnelles;
- Informer toute nouvelle personne employée par Cégep de la présente politique et obtenir son engagement à la respecter;
- Imposer les sanctions appropriées lors de violation des politiques, des règlements, des directives et du code de conduite relatifs à la sécurité de l'information.

Responsable d'actifs informationnels (détenteur)

Chaque direction de service ou de campus assume le rôle de responsable d'actifs informationnels de son service, qu'il 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 son service. Cette personne doit :

- Participer à la catégorisation de l'information de l'unité sous sa responsabilité et à l'analyse de risques;
- Veiller à la protection de l'information et des systèmes d'information en conformité avec la présente politique;
- Rapporter tout événement ou toute menace liée à la sécurité de l'information;
- Collaborer à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information afin de remédier à un incident au besoin.

Utilisatrices et utilisateurs

La responsabilité de la sécurité de l'information du Cégep incombe à toutes les utilisatrices et à tous les utilisateurs des actifs informationnels du Cégep. Toute 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.

À cette fin, cette personne 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 elle-même ou par un tiers, à moins qu'elle démontre que les actions posées par un tiers ne découlent pas d'une négligence ou d'une malveillance de sa part;
- Aviser une personne responsable, un membre du personnel enseignant, sa supérieure immédiate ou son supérieur immédiat de toute situation susceptible de compromettre la sécurité de l'actif informationnel;
- Au besoin, participer à la catégorisation de l'information de son service;
- 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.

CADRE DE GESTION

La mise en œuvre de la présente politique s'appuie sur la définition d'un cadre de gestion en sécurité de l'information qui précise le champ d'action des différentes personnes appelées à intervenir. Le cadre de gestion précise l'organisation fonctionnelle en matière de sécurité de l'information et rend possibles la définition d'objectifs clairs et une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information sont réévaluées 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 risques et des menaces.

La Politique de sécurité de l'information du Cégep se base sur cinq axes fondamentaux de gestion, et son application relève de la cheffe ou du chef de la sécurité de l'information.

Gestion des identités et des accès (GIA)

La gestion des identités et des accès est encadrée et contrôlée pour faire en sorte que seules les personnes autorisées puissent accéder aux informations détenues par le Cégep, les divulguer et les utiliser, ce qui assure ainsi la protection de la confidentialité.

Gestion des vulnérabilités

La gestion des vulnérabilités se caractérise par un déploiement de mesures visant à maintenir à jour les logiciels du parc informatique afin de réduire le plus possible les vulnérabilités et de diminuer les risques d'une cyberattaque. Les fournisseurs ou les prestataires de services doivent mettre en place des mesures de détection des vulnérabilités afin qu'elles soient évaluées et corrigées, le cas échéant.

Gestion des risques

La gestion des risques relatifs à l'actif informationnel du Cégep est basée sur une analyse des menaces liées à l'intégrité, à la disponibilité et à la confidentialité de l'information détenue par le Cégep. De cette analyse découlent des directives reliées à l'utilisation et à l'exploitation des systèmes d'information ainsi qu'aux résultats escomptés.

Gestion des incidents

La gestion des incidents se caractérise par la mise en place de procédures de compte rendu, d'analyse relative aux incidents de sécurité et de mesures correctives pour y donner suite. Les mesures déployées visent à assurer la continuité des services. En gestion des incidents, le Cégep peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'actif informationnel.

Gestion de la reprise et de la continuité des affaires

La gestion de la reprise et de la continuité des affaires se caractérise par l'implantation de processus visant à cibler les incidents opérationnels majeurs qui sont susceptibles de menacer l'établissement tels que les catastrophes naturelles, les pannes d'électricité, de télécommunication ou informatiques, le piratage, le terrorisme, les pandémies, etc. L'identification de ces incidents permet d'évaluer leurs répercussions sur les activités de l'établissement et de mettre en place les mesures d'atténuation nécessaires à la continuité des activités critiques.

FORMATION, SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur l'adoption de 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.

Le Cégep s'engage à sensibiliser et à former régulièrement les utilisatrices et 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 à leurs obligations en la matière. L'utilisatrice et l'utilisateur ont la responsabilité de participer à ces activités de sensibilisation et de formation.

SANCTIONS

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

Toute 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 administratives ou disciplinaires internes applicables.

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

RESPONSABILITÉ DE L'APPLICATION ET RÉVISION DE LA POLITIQUE

La cheffe ou le chef de la sécurité de l'information organisationnelle (CSIO) est responsable de la diffusion et de la mise en application de cette politique. La politique sera révisée au besoin, au minimum tous les cinq ans à compter de sa date d'adoption.

ENTRÉE EN VIGUEUR

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

RÉVISIONS

Date	Action	Version
28 juin 2023	Nouvelle version de la *Politique sur la sécurité de l'information* initialement approuvée par le CA en juin 2017	1.0

RÉFÉRENCES

Aide-mémoire : Politique gouvernementale en cybersécurité

Politique gouvernementale en cybersécurité — Mesures clés