RECUEIL DE GESTION - POLITIQUE

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Adoptée par le conseil d'administration le 14 juin 2022 (Résolution CA-3464)
Amendée par le conseil d'administration le 25 avril 2023 (Résolution CA-3534)

TABLE DES MATIÈRES

1. PRÉAMBULE

La politique sur la sécurité de l'information permet au Cégep de Lévis (ci-après : « Cégep ») d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'il a créée ou reçue. Les différentes informations nécessaires au bon fonctionnement d'un collège sont diversifiées et multiples. Elles consistent en des renseignements nominatifs concernant les étudiants, le personnel et de l'information stratégique ou opérationnelle pour l'administration du collège.

Le monde numérique dans lequel nous évoluons n'a plus de frontières, il est ouvert à la communauté, mais également à des gens mal intentionnés. Ces personnes recherchent les faiblesses des systèmes en place afin d'accéder à nos informations et d'en tirer profit. Notre Cégep, faisant partie du réseau de l'enseignement supérieur, a une image publique et est donc une cible potentielle.

Dans ce contexte, l'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., c. G- 1.03) et de la Directive sur la sécurité de l'information gouvernementale crée des obligations aux établissements collégiaux en leur qualité d'organismes publics. L'adoption de cette politique, sa mise en œuvre, sa mise à jour et son application permet au Cégep de remplir ses obligations.

2. PRINCIPES DIRECTEURS ET VALEURS

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

a) S'assurer de bien connaitre l'information à protéger, en identifier les responsables et leurs caractéristiques de sécurité ;
b) S'appuyer sur les normes pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires ;
c) Adhérer à une approche basée sur le risque acceptable (la mise en place du cadre de gestion de la sécurité de l'information étant un moyen d'ajuster le risque, par une combinaison de mesures raisonnables mises en place pour garantir la sécurité de l'information, à un coût proportionnel à la sensibilité de l'information et aux effets potentiels) ;
d) Reconnaître l'importance de la Politique sur la sécurité de l'information, de son Cadre de gestion et des différents encadrements en matière de sécurité de l'information ;

e) Protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle ;
f) Reconnaître que l'environnement technologique est en changement constant et interconnecté avec le monde ;
g) Évaluer régulièrement les risques, mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, et définir des actions d'éradication des menaces ou de recouvrement des activités compromises ;
h) Protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction ;
i) Adhérer aux principes de partage des meilleures pratiques en matière de sécurité de l'information avec le réseau de l'éducation et des organismes publics ;
j) Adhérer à une démarche éthique visant à former les utilisateurs, pour ensuite assurer la régulation des conduites et la responsabilisation individuelle ;
k) Attribuer les privilèges et droits d'accès qui sont strictement nécessaires pour les activités associées à chaque utilisateur ;
l) Communiquer l'information relative aux menaces pouvant affecter les actifs informationnels, afin que chacun puisse comprendre l'importance d'appliquer la sécurité en plus de reconnaître les incidents et d'agir selon les encadrements en place ;
m) Élaborer et mettre en place un plan de continuité des services essentiels du Cégep.

3. CHAMP D'APPLICATION

La présente politique s'adresse à toute personne physique ou morale, ayant accès, sur place ou à l'extérieur des locaux de l'organisation, aux actifs informationnels desquels un organisme public a la responsabilité d'assurer la sécurité.

L'information visée est celle consignée dans un document et que le Cégep détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

Tous les supports qu'ils soient numériques ou papier, sont concernés.

4. CADRE LÉGAL ET ADMINISTRATIF

La Politique sur la sécurité de l'information s'inscrit principalement dans un contexte réglementaire régi par :

a) La Charte des droits et libertés de la personne (L.R.Q., c. C-12) ;
b) Le Code civil du Québec ;
c) La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics (Décret no 261-2012 du 28 mars 2012);

d) La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement - LGGRI (L.R.Q., c. G-1.03) ;
e) La Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C- 1.1) ;
f) La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1) ;
g) La Loi sur les archives (L.R.Q., c. A-21.1) ;
h) La Directive sur la sécurité de l'information gouvernementale (Décret 7-2014 du 15 janvier 2014);
i) La Loi sur le droit d'auteur (L.R.C., 1985, c. C-42) ;
j) Toutes les politiques et les règlements du Cégep.

5. DÉFINITIONS

a) « Actifs informationnels » : 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 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.

b) « Cadre de gestion » : L'ensemble des consignes, c'est-à-dire les politiques, les règlements, les directives, les procédures et les bonnes pratiques qui encadrent les activités d'un établissement.

c) « CERT/AQ » : Acronyme désignant l'équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale (Computer Emergency Response Team/AreaQuebec).

d) « Confidentialité » : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci .

e) « Document » : Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et 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 transcrits 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 .

f) « 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.

g) « 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.

h) « Plan de continuité » : L'ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité du Cégep.

i) « Responsable d'actifs informationnels » : Membre du personnel cadre détenant la plus haute autorité au sein d'une direction ou d'un service 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 direction ou ce service.

j) « Risque de sécurité de l'information » : Le degré d'exposition d'une information ou d'un système d'information à une menace d'interruption ou de réduction de la qualité des services ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et qui peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ou sur l'image du Cégep.

k) « Utilisateur » : Tout membre de la communauté étudiante, du personnel ou personne physique autorisée qui accède par l'entremise des réseaux numérique et non numérique aux actifs informationnels du Cégep.

6. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Cégep à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information détenue et traitée par le Cégep, quels que soient son support ou ses moyens de communication et ce à toutes les étapes de son cycle de vie.

Plus précisément le Cégep doit :

- S'assurer que l'information soit disponible et accessible en temps voulu et de la manière requise aux personnes autorisées ;
- Préserver l'intégrité de l'information de manière que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues ;
- S'assurer de la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, de façon plus spécifique pour les renseignements personnels.

Par conséquent, le Cégep met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée par le Cadre de gestion de la sécurité de l'information. Ce cadre renforce les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales.

7. CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

La politique confère la reconnaissance et la légitimité à la direction de définir des directives, des procédures et des guides en lien avec la sécurité de l'information. L'ensemble de ces documents font partie du cadre de gestion qui viendra préciser les actions permettant l'atteinte des objectifs de la présente politique.

8. 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.

8.1 Conseil d'administration

Le conseil d'administration adopte la Politique sur la sécurité de l'information ainsi que toute modification à celle-ci. Le conseil est régulièrement informé des actions du Cégep en matière de sécurité de l'information. Il est le dirigeant de l'organisme responsable de l'application de la Politique sur la sécurité de l'information.

8.2 Comité de direction

Le comité de direction du Cégep détermine des mesures visant à favoriser l'application de la politique et des obligations légales du Cégep en matière de sécurité de l'information. Ainsi, il en approuve les orientations stratégiques et peut également définir des directives et des procédures qui viendront préciser ou soutenir l'application de la politique.

8.3 Comité en sécurité de l'information

Ce comité de travail a comme objectif d'assister le chef de la sécurité de l'information organisationnelle (CSIO) afin de définir et mettre en place le Cadre de gestion de la sécurité de l'information, les plans d'action, les activités de sensibilisation ou de formation ainsi que tout autre élément pouvant être nécessaire pour assurer la protection du Cégep et être conforme à la réglementation.

Le comité est formé du CSIO qui en assure l'animation, de la personne responsable de l'application de la Loi sur l'accès aux documents des organismes publics et de la protection des renseignements personnels, des coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI), de la direction des services des technologies de l'information et des immeubles et d'une personne responsable de la gestion documentaire du Cégep. Le comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses activités.

8.4 Comité de crise en sécurité de l'information

En cas d'incident critique de sécurité informatique, le Comité en sécurité de l'information se joindra au Comité de direction afin de constituer le comité de crise en sécurité de l'information sous la responsabilité de la direction générale. Ce comité est le groupe décisionnel appelé à intervenir notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services.

Il a pour rôle :

- D'autoriser la mise en œuvre de stratégies permettant d'assurer la prise en charge des incidents critiques de sécurité de l'information ;
- De formuler des recommandations concernant le délestage, en totalité ou en partie, des activités de l'organisation ;
- De communiquer avec la communauté et les médias.

Ce comité peut s'adjoindre toute autre personne en mesure de lui assurer le soutien adéquat dans le cadre de ses prises de décision.

8.5 Direction générale

La direction générale veille à l'application de la Politique sur la sécurité de l'information.

Elle aura pour tâche :

- D'encadrer le CSIO dans la réalisation de son mandat ;
- D'autoriser les redditions de comptes en matière de sécurité de l'information ;
- D'autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission du Cégep ;
- D'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique ;
- De tenir à jour le registre des dérogations et le registre des cas de contravention à la présente politique ;
- De diriger le comité de crise en sécurité de l'information.

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

La fonction du CSIO est déléguée par le conseil d'administration à une personne cadre. Le CSIO relève de la direction générale au sens du Cadre gouvernemental de gestion de la sécurité de l'information.

Le CSIO assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. Il travaille en étroite collaboration avec les répondants en matière de sécurité de l'information pour assurer la prise en charge des exigences de sécurité de l'information.

Il assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

- Mettre en œuvre les décisions émanant du chef gouvernemental de la sécurité de l'information (CGSI) et du chef délégué de la sécurité de l'information (CDSI) auquel il se rattache, notamment les indications d'application et les indications d'application particulières, en coordonner l'exécution et veiller à leur application ;
- Contribuer à la mise en œuvre du cadre de gouvernance qui régit la sécurité de l'information au sein de son organisation ;

- Contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de gestion de la sécurité de l'information et des processus de sécurité de l'information élaborés par le chef délégué de la sécurité de l'information (CDSI) ;
- S'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement, d'acquisition, d'évolution ou de remplacement d'un actif informationnel ou d'un service en ressources informationnelles ;
- Aviser sans délai le chef délégué de la sécurité de l'information (CDSI) lorsqu'un événement de sécurité présente un risque qu'un préjudice sérieux soit causé ;
- Mettre en œuvre les actions requises pour la prise en charge d'un événement de sécurité ;
- Tenir un registre des événements de sécurité selon les exigences de la Directive et les modalités précisées par le chef délégué de la sécurité de l'information (CDSI) ;
- Fournir les informations demandées par le chef gouvernemental de la sécurité de l'information (CGSI) et le chef délégué de la sécurité de l'information (CDSI) auquel il se rattache relativement à la reddition de comptes, ou toute autre information requise par ces derniers ;
- Mettre en place au sein de son organisation les comités et les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination ;
- Assurer le développement des compétences du personnel de son organisation en matière de sécurité de l'information.

8.7 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) est responsable de l'application du processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) pour le cégep, en soutien à son chef de la sécurité de l'information organisationnelle (CSIO).

En plus de ces responsabilités, le COMSI doit :

- représenter le cégep et participer activement au Réseau d'alerte gouvernemental, coordonné par le CERT/AQ ;
- identifier les menaces, vulnérabilités et incidents (MVI) touchant le cégep, en tenir informé son CSIO et les faire remonter selon les conditions définies par le processus GMVI, si nécessaire ;
- s'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux MVI ;
- s'assurer de la réalisation d'analyses de risques de sécurité ;

- collaborer étroitement avec son CSIO et son responsable opérationnel de cyberdéfense (ROCD) en leur fournissant, notamment, le soutien technique nécessaire à l'exercice de leurs responsabilités.

8.8 Direction des Services des technologies de l'information et des immeubles

8.8.1 Service des technologies de l'information

En matière de sécurité de l'information, le service des technologies de l'information s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels il intervient :

- Il participe 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 ;
- Il applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, telles que par exemple l'interruption ou la révocation temporaire - lorsque les circonstances l'exigent - des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause ;
- Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la direction générale.

8.8.2 Service des immeubles

Le service des immeubles participe, avec le CSIO, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

8.9 Responsable d'actifs informationnels

La personne responsable d'actifs informationnels peut déléguer la totalité ou une partie de sa responsabilité à un autre membre du service.

Cette personne :

- Informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de la politique de sécurité de l'information et des dispositions du Cadre de gestion de la sécurité de l'information dans le but de le sensibiliser à la nécessité de s'y conformer ;

- Collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques ;
- Voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la politique de sécurité de l'information et de tout autre élément du cadre de gestion ;
- S'assure 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 voit à ce que tout(e) 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 ;
- Rapporte au service des technologies de l'information toute menace ou tout incident afférant à la sécurité de l'information ;
- Collabore 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 ;
- Rapporte à la direction générale tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette politique.

8.10 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 ;
- 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, au besoin, à la catégorisation de l'information de son service ;
- Respecter les mesures de sécurité mises en place, ne pas les contourner, modifier leur configuration ou les désactiver ;
- Signaler à la personne responsable des actifs informationnels 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 ;

- 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; Aussi, tout utilisateur du Cégep doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

9. SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et 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 leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. De plus, des documents explicatifs sont disponibles à l'ensemble des utilisateurs.

10. SANCTIONS

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, sur décision de l'autorité hiérarchique compétente et dans le respect des conventions collectives et de tout contrat de travail, 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.

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.

11. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le CSIO, est responsable de la diffusion et de la mise à jour de la politique.

12. ENTRÉE EN VIGUEUR ET RÉVISION

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration, soit le 14 juin 2022.

La Politique sur la sécurité de l'information est révisée à chaque trois (3) ans et modifiée au besoin, notamment lorsque des modifications législatives le requiert