Cégep de l'Abitibi-Témiscamingue

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Responsable : Direction générale

Dernière mise à jour : 14 septembre 2021

ADOPTION PAR LE CONSEIL D'ADMINISTRATION

25 septembre 2018

AMENDEMENTS

14 septembre 2021

TABLE DES MATIÈRES

PRÉAMBULE

La *Politique de sécurité de l'information* permet au Cégep de l'Abitibi-Témiscamingue de respecter les lois et de réduire les risques en protégeant l'information qu'il a créée ou reçue. Cette information est multiple et diversifiée. Elle comprend des renseignements personnels d'étudiants, d'étudiantes et de membres du personnel, de l'information professionnelle sujette à des droits de propriété intellectuelle et, finalement, de l'information stratégique ou opérationnelle pour l'administration du Cégep.

Le monde d'aujourd'hui n'a plus de frontières, il est ouvert à des pirates modernes en quête d'argent ou de prestige. Ces pirates, cachés dans un espace numérique parfois proche, parfois très éloigné, recherchent les faiblesses des systèmes en place pour réussir à accéder à notre information. 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 (RLRQ,* chapitre G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale* (une directive du Conseil du trésor du Québec applicable aux cégeps) créent des obligations aux établissements collégiaux en leur qualité d'organismes publics. Ainsi, la *Directive sur la sécurité de l'information gouvernementale* oblige le Cégep à adopter, à mettre en œuvre, à mettre à jour et à s'assurer de l'application d'une *Politique de sécurité de l'information* – dont les principales modalités sont définies dans la directive gouvernementale – en ayant recours notamment à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

1. Définitions

a) **Actifs informationnels :** Inventaire présentant, à un moment déterminé, le portrait de l'ensemble des ressources informationnelles d'une entreprise ou d'une organisation, à l'exception des ressources humaines.

b) ***Cégep :*** Le Cégep (Collège d'enseignement général et professionnel) de l'Abitibi-Témiscamingue.

c) ***Loi :*** *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) (RLRQ, chapitre G-1.03).*

d) ***Membre du personnel :*** Le personnel enseignant, professionnel, de soutien et cadre.

e) ***Personne*** **:** Les personnes qui étudient, travaillent, visitent ou fréquentent de quelque façon que ce soit le Cégep.

f) ***Population étudiante*** *:* Les étudiantes et les étudiants dûment inscrits au Cégep.

2. Principes directeurs

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

a) La reconnaissance de l'importance d'assurer la sécurité de l'information.

b) La connaissance de l'information à protéger.

c) L'application des normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou des établissements similaires.

d) Une approche basée sur le risque acceptable (la mise en place du cadre de gestion est 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).

e) La protection rigoureuse des renseignements personnels ainsi que de toute autre information confidentielle.

f) La reconnaissance que l'environnement technologique est en changement constant et interconnecté avec le monde (en mettant en place une gestion de la sécurité de l'information qui s'adapte à ces changements).

g) La reconnaissance de l'importance d'évaluer régulièrement les risques, de mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, de définir des actions d'éradication des menaces ou de recouvrement des activités compromises.

h) La protection de 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 (le niveau de sécurité pouvant varier au cours du cycle de vie du document).

i) Le partage des meilleures pratiques et la gestion de l'information opérationnelle en matière de sécurité de l'information avec le réseau de l'éducation et les autres organismes publics.

j) Une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle (chaque individu qui a accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci).

k) L'accès, pour chaque membre du personnel, au minimum d'information requis pour accomplir ses tâches normales.

l) L'accès, pour la population étudiante, à l'information requise pour la réussite de son projet d'études.

m) La transparence, au sujet des menaces pouvant affecter les actifs informationnels afin que chacun puisse comprendre l'importance d'appliquer les consignes de sécurité demandées et que chacun puisse reconnaître les incidents de sécurité et agir en conséquence.

3. 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, quels que soient son support ou ses moyens de communication. Plus précisément, le Cégep doit veiller à :

a) La disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées.

b) L'accessibilité pour les enseignants, à un environnement technologique favorisant la qualité des activités d'apprentissage dans le respect de la sécurité de l'information.

c) L'intégrité de l'information de manière à ce 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.

d) La confidentialité de l'information en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout s'il s'agit de renseignements personnels.

e) La mise en place d'un plan de continuité des affaires en vue de rétablir les services essentiels à sa clientèle selon un temps prévu.

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

4. Cadre légal et administratif

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

a) La *Charte des droits et libertés de la personne* (RLRQ, chapitre C-12).

b) Le *Code civil du Québec* (CCQ, 1991).

c) La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*.

d) La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, chapitre G-1.03).

e) La *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, chapitre C-1.1).

f) La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1).

g) La *Loi sur les archives* (RLRQ, chapitre A-21.1).

h) Le *Code criminel* (LRC, 1985, chapitre C-46).

i) Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, r. 2).

j) La *Directive sur la sécurité de l'information gouvernementale.*

k) La *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42).

5. Champ d'application

La présente *Politique* s'adresse aux utilisateurs et aux utilisatrices de l'information, c'est-à-dire à tous les membres du personnel, à toute personne physique ou morale qui, à titre de consultant, de partenaire, de fournisseur, d'étudiant ou d'étudiante ou de public, utilisent les actifs informationnels du Cégep.

L'information visée est celle 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, incluant le papier, sont concernés.

6. Gestion des accès

Chaque système d'information peut représenter un risque. Alors, le droit d'accès d'un utilisateur ou d'une utilisatrice aux divers systèmes est attribué en fonction de ce qui est nécessaire pour l'exécution des tâches qu'il a à accomplir. Chaque demande d'accès fait l'objet d'une autorisation formelle par une autorité supérieure. Respectant le principe d'imputabilité, la règle générale inhérente à l'attribution d'un code d'accès est : un utilisateur ou une utilisatrice se voit attribuer un code d'accès personnel. Aucun code d'accès générique ne sera accordé.

Un code d'accès individuel est alloué à un utilisateur ou une utilisatrice par le Cégep à titre personnel et confidentiel. Il en est de même pour le mot de passe. L'utilisateur ou l'utilisatrice est responsable des communications ou des actions sur le réseau utilisant des applications initiées par l'utilisation de son code d'accès et de son mot de passe : de ce fait, il a la

responsabilité de les protéger. En aucun cas l'utilisateur ou l'utilisatrice ne doit divulguer son mot de passe.

Dans une perspective de sécurité et afin de répondre aux normes actuelles en matière de sécurité, seuls les mots de passe respectant les critères établis par le Cégep seront acceptés pour l'authentification sur le réseau et dans les systèmes de gestion.

Un registre est tenu à jour pour décrire la liste des fournisseurs ou mandataires bénéficiant d'un accès à distance ou non au réseau.

Par le biais d'une procédure à cet effet, le Cégep détermine la durée des accès à un ou plusieurs outils informatiques lorsqu'il y a une modification au lien d'emploi d'un membre du personnel, qu'il s'agisse d'un départ à la retraite, d'un départ pour un autre emploi ou de toute autre situation.

7. 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.

7.1. Conseil d'administration

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

Le conseil d'administration nomme par résolution le responsable de la sécurité de l'information (RSI).

7.2. Comité de direction

Le comité de direction du Cégep détermine, au besoin, des mesures visant à l'application de la *Politique* et des obligations légales du Cégep en matière de sécurité de l'information. Il valide la *Politique* ainsi que ses mises à jour.

7.3. Comité de travail sur la sécurité de l'information

Le comité de travail sur la sécurité de l'information a comme objectif d'assister le responsable de la sécurité de l'information (RSI) à mettre en place les éléments pouvant être nécessaires pour assurer la protection du Cégep afin qu'il soit conforme à la réglementation. Le comité sera formé des parties prenantes du Cégep qui seront directement concernées ou qui participent au projet de mise en place de la sécurité de l'information.

7.4. Directeur général ou directrice générale

Le directeur général ou la directrice générale est responsable de la mise en place et de l'application de la *Politique de sécurité de l'information*.

Cette personne aura pour tâche :

a) D'encadrer et de soutenir le ou la responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat.

b) De fournir les ressources et les outils nécessaires à la mise en place du Cadre de gestion de la sécurité de l'information.

c) D'autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions d'une directive ou d'une procédure institutionnelle liées à la sécurité de l'information et 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) D'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la *Politique*.

e) De maintenir à jour le registre des dérogations et le registre des cas de contravention à la présente *Politique.*

f) De définir la composition du comité de travail sur la sécurité de l'information.

7.5. Responsable de la sécurité de l'information (RSI)

La fonction du ou de la RSI est déléguée à une personne-cadre par le conseil d'administration. Le ou la RSI relève du directeur général ou de la directrice générale au sens du *Cadre gouvernemental de gestion de la sécurité de l'information*. Cette personne met en place le *Cadre de gestion de la sécurité de l'information* et s'assure que le niveau de maturité en gestion de la sécurité de l'information réponde aux besoins. Elle est nommée par le conseil d'administration.

Le ou la RSI :

a) Élabore et propose le programme de sécurité de l'information du Cégep. Il ou elle rend compte de son implantation au comité de direction.

b) Formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et met à jour la *Politique*.

c) Assure la coordination et la cohérence des actions menées au sein du Cégep en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans les unités.

d) Produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information.

e) Propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats.

f) S'assure de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale (Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale (CERT/AQ)).

g) Collabore à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille au déploiement de ceux-ci.

h) Procède aux enquêtes lors de transgressions sérieuses ayant trait présumément à la *Politique* à la suite de l'autorisation du directeur général ou de la directrice générale.

i) S'assure des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

j) Identifie les rôles et responsabilités des personnes responsables des actifs informationnels.

7.6. Service des technologies de l'information et de l'audiovisuel

En matière de sécurité de l'information, le Service des technologies de l'information et de l'audiovisuel 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 :

a) 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.

b) 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.

c) Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente *Politique* et autorisées par le directeur général ou la directrice générale.

7.7. Direction des services financiers et de l'approvisionnement et Direction des ressources matérielles

La Direction des services financiers et de l'approvisionnement informe les fournisseurs et les entrepreneurs qui doivent accéder à l'infrastructure technologique de l'importance de l'application de la *Politique de la sécurité de l'information* et leur fait signer un engagement au respect de cette *Politique* (annexe 1).

Le Direction des ressources matérielles, en collaboration avec le ou la responsable de la sécurité de l'information, procède à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

7.8. Direction des ressources humaines

La Direction des ressources humaines informe chaque membre du personnel, lors de sa nomination, de l'importance de l'application de la *Politique de la sécurité de l'information* et lui fait signer un engagement au respect de cette *Politique* (annexe 1).

7.9. Direction des affaires étudiantes et des communications

La Direction des affaires étudiantes et des communications informe la population étudiante de l'importance de l'application de la *Politique de la sécurité de l'information* et s'assure que tous les étudiants et toutes les étudiantes ont signé un engagement à cet effet.

7.10. Responsable d'actifs informationnels

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

Les droits du ou de la responsable d'actifs informationnels sont identifiés par le ou la RSI.

Le ou la responsable d'actifs informationnels :

a) Informe les membres du 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 dans le but de le sensibiliser à la nécessité de s'y conformer.

b) Collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques.

c) 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 les membres du personnel relevant de son autorité en conformité avec la *Politique de sécurité de l'information* et de tout autre élément du cadre de gestion.

d) 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 consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la *Politique* et tout autre élément du cadre de gestion.

e) Rapporte au Service des technologies de l'information et de l'audiovisuel toute menace ou tout incident afférent à la sécurité de l'information.

f) 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.

g) Rapporte au ou à la RSI 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.*

7.11. Utilisateurs ou utilisatrices

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

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

À cette fin, l'utilisateur ou l'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) 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.

c) Participer à la catégorisation de l'information de son service.

d) Respecter les mesures de sécurité mises en place, ne pas les contourner, ni modifier leur configuration, ni les désactiver.

e) Signaler au ou à la 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.

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

8. Sensibilisation et information

La sécurité de l'information repose notamment sur l'utilisation de bonnes pratiques 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 sur le site Internet du Cégep.

9. Sanctions

En cas de contravention à la présente *Politique*, l'utilisateur ou l'utilisatrice 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.

9.1. Mesures administratives ou disciplinaires

Selon les impacts et la gravité, en cas de manquement à la présente *Politique* par la communauté collégiale, les modalités prévues aux conventions collectives du personnel, les modalités prévues à la *Politique de gestion définissant les conditions d'engagement et d'emploi du personnel d'encadrement*, le *Règlement relatif au code de conduite à l'intention de la population étudiante,* ou les modalités prévues aux baux des locataires s'appliqueront.

Également, en cas de manquement à la présente *Politique* par les personnes qui visitent ou fréquentent le Cégep, ce dernier se réserve le droit d'appliquer des mesures administratives pouvant aller jusqu'à l'expulsion.

10. Diffusion et mise à jour de la Politique

La personne responsable de la sécurité de l'information, assistée du comité de travail sur la sécurité de l'information, est responsable de la diffusion et de la mise à jour de la *Politique*.

11. Entrée en vigueur et révision

11.1. Entrée en vigueur

La présente *Politique* entre en vigueur à la date de son adoption par le conseil d'administration, soit le 25 septembre 2018.

11.2. Révision

La *Politique de sécurité de l'information* sera révisée au plus tard trois ans après son adoption.

ANNEXE I

Engagement au respect de la *Politique de sécurité de l'information*

Cégep de l'Abitibi-Témiscamingue

Conformément à *la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* et à la *Directive sur la sécurité de l'information gouvernementale*, le Cégep de l'Abitibi-Témiscamingue a adopté une *Politique de sécurité de l'information* qui identifie notamment des processus formels de sécurité de l'information afin d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Je déclare avoir pris connaissance de la *Politique de sécurité de l'information du Cégep de l'Abitibi-Témiscamingue* et je reconnais avoir l'obligation de respecter ces dispositions.

Je m'engage à :

- Me 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 me sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à ma disposition uniquement dans le cadre de mes fonctions ou de mes activités qui sont en lien avec le Cégep 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.
- Signaler au Service des technologies de l'information et de l'audiovisuel du Cégep, tout incident susceptible de constituer une infraction à la présente *Politique* ou de constituer une menace à la sécurité de l'information du Cégep (au poste 1-811 ou à l'adresse courriel : support@cegepat.qc.ca)
- 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.

Fait à : _____ , ce _____ 20 ____

Signature _____

Membre du personnel ☐ Étudiant ou étudiante ☐

Nom : _____
(En lettres moulées)

Entreprises, fournisseurs ou organisations susceptibles d'accéder à l'infrastructure technologique du Cégep de l'Abitibi-Témiscamingue

Nom de l'entreprise, du fournisseur ou de l'organisation _____ Rôle ou fonction _____

Fait à _____ , ce _____ 20 ____

Signature _____

Nom _____
(En lettres moulées)