Cégep de l'Outaouais

DSA-P4

CA 555.16
2022 02 15

POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

DU CÉGEP DE L'OUTAOUAIS

Notes chronologiques

Politique relative à la sécurité de l'information adoptée le 15 février 2022.

Politique adoptée en vertu de :

Voir article 3 de la présente politique

Table des matières

Préambule..... 3

Article 1 Définitions 3

Article 2 Objectifs 3

Article 3 Cadre légal et administratif 4

Article 4 Champs d'application 4

Article 5 Énoncés de principes généraux 4

Protection de l'information 4

Engagement des utilisateurs 4

Protection des renseignements confidentiels 4

Sensibilisation et formation 5

Droit de regard 5

Article 6 Axes de gestion de la sécurité de l'information 5

6.1 Gestion des accès 5

6.2 Gestion des risques 5

6.3 Gestion des incidents 5

Article 7 Obligations et responsabilités des intervenants clés en matière de sécurité de l'information 6

Le conseil d'administration 6

Le directeur général 6

Responsable de la sécurité de l'information (RSI) 6

Coordonnatrice ou Coordonnateur sectoriel de la gestion des incidents (CSGI) 6

Service de l'informatique, multimédia et reprographie (SIMeR) 6

Centre Collégiale de transfert technologique (CCTT) CyberQuébec 7

Service des ressources matérielles 7

Direction des ressources humaines 7

Détenteur d'actifs informationnels 7

Les utilisateurs 8

Article 8 Sanctions 8

Article 9 Dispositions finales 8

Préambule

La Politique de sécurité de l'information établit les balises nécessaires à la protection de l'information créée, reçue et détenue par le Cégep de l'Outaouais dans le cadre de ses activités. Il s'agit, notamment, des renseignements personnels d'étudiantes et d'étudiants, de membres du personnel et de tierces parties,de l'information professionnelle sujette à des droits de propriété intellectuelle et d'informations stratégiques ou opérationnelles utilisées pour l'administration du Cégep.
Par la présente politique, le Cégep se conforme 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 faisant état des obligations auxquelles doivent se conformer tous les organismes publics quant à l'adoption, à la mise en œuvre et au suivi de l'application d'une politique de sécurité de l'information.

Article 1 Définitions

Actif informationnel – La *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., chapitre C-1.1) définit l'actif informationnel sans égard au support comme étant : « 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 elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles. » Cette même loi assimile 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.

Confidentialité – Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Cycle de vie de l'information – L'ensemble des étapes que franchit une information et qui vont de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou à sa destruction, en conformité avec le calendrier de conservation[1].

Disponibilité – Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

Intégrité – Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité

Article 2 Objectifs

La présente politique a pour objectif de définir les balises permettant au Cégep de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient les supports ou les moyens de communication utilisés.

Plus précisément, le Cégep doit veiller :

- à assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées ;
- à assurer 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 utilisé offre la stabilité et la pérennité voulues ;
- à assurer la confidentialité de l'information en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées et aux fins prévues

[1] Pour les références au calendrier de conservation, voir la Politique de gestion des documents administratifs et des archives DCAC – P3.

Article 3 Cadre légal et administratif

La présente politique s'inscrit principalement dans un contexte régi par les lois et documents suivants

- *Charte des droits et libertés de la personne* (LRQ, chapitre C-12) ;
- *Code civil du Québec* (LQ, 1991, chapitre 64) ;
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03) ;
- *Loi concernant le cadre juridique des technologies et l'information* (LRQ, chapitre C-1.1) ;
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1) ;
- *Loi sur les archives* (LRQ, chapitre A-21.1) ;
- *Loi sur l'administration publique* (LRQ, chapitre A-6.01) ;
- *Loi sur la fonction publique* (LRQ, chapitre F-3.1.1) ;
- *Loi canadienne sur les droits de la personne* (LRC. (1985), chapitre H-6) ;
- *Code criminel* (LRC. (1985), chapitre C-46) ;
- *Loi sur le droit d'auteur* (LRC. (1985), chapitre C-42) ;
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2) ;
- Directive sur la sécurité de l'information gouvernementale

Article 4 Champs d'application

La présente politique s'applique aux utilisateurs, c'est-à-dire à tous les membres du personnel, peu importe leur statut, et à toute personne physique ou morale qui, à titre d'employée ou employé, de consultante ou consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du Cégep ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que le Cégep détient dans la réalisation de ses opérations, et ce, qu'il en assure la conservation ou que celle-ci soit assurée par un tiers.

Article 5 Énoncés de principes généraux

Protection de l'information
Le Cégep de l'Outaouais adhère aux orientations et aux objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'à l'échelle internationale.

Le Cégep reconnaît que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, qu'ils doivent faire l'objet d'une évaluation constante, d'une gestion des risques, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection dont les actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ils sont exposés.

La sécurité des actifs informationnels s'inscrit dans une préoccupation éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

Engagement des utilisateurs
La protection de l'information détenue par le Cégep s'appuie sur l'engagement continu de l'ensemble des utilisatrices et utilisateurs. Chacun a l'obligation de protéger l'information et le matériel mis à sa disposition. Les utilisatrices et les utilisateurs ont des responsabilités explicites en matière de sécurité et sont redevables de leurs actions.

Protection des renseignements confidentiels
Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée. Sont notamment considérés comme confidentiels, au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences, notamment sur les relations intergouvernementales, les négociations entre organismes publics,

l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et la sécurité publique, les décisions administratives ou politiques et la vérification.

Sensibilisation et formation
Le Cégep s'engage, sur une base régulière, à sensibiliser et à former les utilisatrices et les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et à leurs obligations en la matière.

Droit de regard
Le Cégep exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage de ses actifs informationnels et des moyens qui permettent d'y accéder.

Article 6 Axes de gestion de la sécurité de l'information

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents acteurs du Cégep permettant une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être remises en question de manière périodique afin 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 trois axes fondamentaux de gestion. Ces axes sont la gestion des accès, la gestion des risques et la gestion des incidents.

6.1 Gestion des accès

La gestion des accès doit être encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le dessein de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités à tous les membres du personnel et sur l'obligation pour chacun d'eux d'en rendre compte selon leur fonction au sein du Cégep

6.2 Gestion des risques

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse de risques guide également l'acquisition, la conception et l'exploitation des systèmes d'information en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du Cégep. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Cégep. Les risques à portée gouvernementale sont déclarés, conformément à la Directive sur la sécurité de l'information gouvernementale.

Le niveau de protection de l'information est établi en fonction :

- de la nature de l'information et de son importance ;
- des probabilités d'accident, d'erreur ou de malveillance auxquels elle est exposée ;
- des conséquences de la matérialisation de ces risques ;
- du niveau de risque acceptable selon le Cégep.

6.3 Gestion des incidents

Le Cégep déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires à l'atteinte des buts suivants :

- limiter l'occurrence des incidents en matière de sécurité de l'information ;
- gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés conformément à la Directive sur la sécurité de l'information gouvernementale. Dans la gestion des incidents, le Cégep peut exercer ses pouvoirs et ses prérogatives en ce qui a trait à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

Article 7 Obligations et responsabilités des intervenants clés en matière de sécurité de l'information

La présente politique détermine les obligations en matière de sécurité de l'information attribuées, notamment, au responsable organisationnel de la sécurité de l'information, aux gestionnaires d'entités administratives et aux utilisatrices et utilisateurs.

Le conseil d'administration
Le conseil d'administration approuve la présente politique ainsi que ses mises à jour et autorise la nomination du responsable de la sécurité de l'information (RSI).

Le directeur général
La directrice ou le directeur général est le premier responsable de la sécurité de l'information relevant de son autorité et assure la mise en œuvre de la présente politique. Il encadre le RSI dans la réalisation de son mandat.

Responsable de la sécurité de l'information (RSI)
La personne RSI relève de la directrice ou directeur général 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 répond aux besoins. Elle est nommée par le conseil d'administration. Elle a pour fonction de soumettre à la direction générale de son organisation les orientations, les politiques, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la SI de son organisation.

Elle contribue, avec ses CSGI (coordonnateur sectoriel de la gestion des incidents en sécurité de l'information [SI]), à la mise en place d'un processus formel de gestion et de déclaration des incidents, incluant un registre des incidents et d'en assurer la mise en œuvre dans son organisation.

Elle assure la coordination et la cohérence des actions de la SI menées au sein de son organisation par d'autres acteurs, tels que les détenteurs de l'information ainsi que les unités responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire et de la sécurité physique des supports d'archivage.

Elle s'assure que des dispositions visant le respect des exigences en matière de sécurité de l'information sont intégrées dans les ententes de service et les contrats.

Elle participe aux enquêtes dans des transgressions sérieuses ayant trait à la politique.

Coordonnatrice ou Coordonnateur sectoriel de la gestion des incidents (CSGI)
La ou le CSGI apporte son soutien au RSI du Cégep, notamment en ce qui a trait à la gestion des incidents et des risques en SI. Il est l'interlocuteur officiel du Cégep auprès du CERT/AQ. Il collabore auprès du RSI du Cégep à l'élaboration des divers éléments stratégiques et tactiques en SI tels que :

- Une politique de SI;
- Un cadre de gestion;
- Un registre d'autorité;
- La catégorisation des actifs;
- Des mesures de sécurité pour les actifs critiques ;
- Un processus formel de gestion des risques en SI ;
- Un processus formel de gestion des droits d'accès à l'information;
- Un processus formel de gestion et de déclaration des incidents de son organisme incluant un registre des incidents de son organisation;

Service de l'informatique, multimédia et reprographie (SIMeR)
En matière de sécurité de l'information, le SIMeR 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, avec les autres intervenantes ou intervenants, 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 participe à l'analyse des mesures à mettre en œuvre dans les trois axes de gestion de la sécurité de l'information : la gestion des accès, la gestion des risques et la gestion des incidents.

Il applique des mesures de réaction appropriées à toute menace et à tout incident de sécurité de l'information, tels 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.

Centre Collégiale de transfert technologique (CCTT) CyberQuébec
Par son expertise en sécurité de l'information, le CCTT joue le rôle d'expert en sécurité de l'information pour le Cégep de l'Outaouais.

Il participe 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 joue un rôle conseil dans la mise en place de solutions appropriées afin de mieux prévenir et de mieux réagir aux menaces et incidents de sécurité de l'information.

Service des ressources matérielles
Il participe, avec la personne RSI et les CSGI, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

Le service des ressources matérielles participe aux enquêtes relatives à des contraventions réelles ou apparentes à la présente politique.

Direction des ressources humaines
En matière de sécurité de l'information, la direction des ressources humaines obtient de tout nouvel employé ou employée du Cégep, après lui en avoir montré la nécessité, son engagement au respect de la politique.

Il organise des activités de sensibilisation et des séances de formation au personnel du Cégep face à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en cette matière.

Détenteur d'actifs informationnels
Le personnel d'encadrement est le détenteur d'actifs informationnels dans son champ de responsabilités. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous sa responsabilité. Il peut donc y avoir plusieurs détenteurs d'actifs informationnels au Cégep. Par ailleurs, il ne doit y avoir qu'un seul détenteur par actif informationnel. Le détenteur d'actif informationnels peut déléguer sa responsabilité du point de vue opérationnel. Cependant, il demeurera responsable de l'accessibilité, de l'utilisation adéquate et de la sécurité de celui-ci.

Le détenteur d'actifs informationnels 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 dans le but de le sensibiliser à la nécessité de s'y conformer.

Il collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques. Il 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.

Il 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 consultante ou consultant, fournisseur, partenaire, invitée ou invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion.

Il rapporte au SIMeR toute menace ou tout incident afférant à la sécurité de l'information. Il 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.

Il rapporte à la directrice ou au directeur général toutes contraventions ou tous problèmes liés 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.

Les utilisateurs
Tout utilisatrice ou utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le Cégep.

À cette fin, il doit :

- prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et s'y conformer ;
- dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, utiliser les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés ;
- respecter les mesures de sécurité mises en place sur son poste de travail et sur tout appareil contenant des données à protéger et ne pas modifier leur configuration ni les désactiver ;
- se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister ;
- signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du Cégep ;
- au moment de son départ du Cégep, remettre les actifs informationnels ainsi que tout le matériel informatique ou de téléphonie mis à sa disposition dans le cadre de l'exercice de ses fonctions.

Article 8 Sanctions

Tout membre de la communauté collégiale qui contrevient à la présente politique s'expose 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, dont celles des conventions collectives, des ententes ou des contrats.

Le Cégep peut transmettre à toute autorité judiciaire les renseignements colligés et qui portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

Article 9 Dispositions finales

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration et est révisée à la demande de la Direction générale.