CÉGEP ÉDOUARD MONTPETIT

Politique de sécurité de l'information et des technologies

Adoptée le 17 février 2015

Amendée en date du 30 novembre 2022

Versions	Date	Par	Type	Changements
1.0	17-02-2015	- Normand Guilbault - Amar Lakhdari	Création	Création et adoption par le conseil d'administration
2.0	08-09-2022	- Jim Morrison Lafrenière, directeur adjoint, transformation numérique et cybersécurité, Direction des systèmes et technologie de l'information - Erick Tayouo, analyste, Direction des systèmes et technologie de l'information - Michel Vincent, directeur, Direction des systèmes et technologie de l'information	Amendement	Toutes les parties
2.1	10-11-2022	- Marie-Pier Lépine, secrétaire générale, Direction générale - Benoît Themens, analyste, Direction générale - Jim Morrison Lafrenière, directeur adjoint, transformation numérique et cybersécurité, Direction des systèmes et technologie de l'information	Validation	Les parties amendées
2.2	30-11-2022	- Jim Morrison Lafrenière, directeur adjoint, transformation numérique et cybersécurité, Direction des systèmes et technologie de l'information	Approbation	Présentation de la version finale pour approbation aux membres du CA

Table des matières

1. Préambule

L'émergence et l'accroissement rapide des technologies de l'information dans la société en général et dans le milieu de l'enseignement en particulier ont entrainé l'introduction graduelle de nombreux équipements et technologies au cégep Édouard-Montpetit ainsi que l'expansion rapide de l'infrastructure de réseau, incluant les technologies gérées depuis l'infonuagique.

Sur cette infrastructure transite principalement de l'information sensible et confidentielle tel que :

- Des renseignements personnels sur les membres de la population étudiante et les membres du personnel et des informations diverses ayant une valeur légale, administrative ou économique;
- Des productions littéraires et du matériel didactique assujettis aux lois sur la propriété intellectuelle;
- Des informations et des dossiers de gestion nécessaires aux opérations quotidiennes du Cégep.

Nous savons par ailleurs que plusieurs lois et directives encadrent et régissent l'utilisation de l'information; le cégep Édouard-Montpetit étant assujetti à ces lois, il se doit d'en assurer le respect.

La direction du Cégep reconnaît que l'information est essentielle à ses opérations courantes, mais que celle-ci doit être utilisée de façon appropriée et bénéficier d'une protection adéquate.

C'est dans ce contexte que le Cégep met en place la présente Politique qui oriente et détermine l'utilisation appropriée et sécuritaire de l'information et des technologies sur lesquelles elle transige.

2. Cadre légal et administratif

Le cadre légal et administratif de la présente Politique est constitué principalement par les lois canadiennes et québécoises en vigueur.

À cet effet, tout utilisateur, tel que défini dans la section 3, qui est appelé à utiliser, à gérer ou à traiter les actifs informationnels du cégep Édouard-Montpetit doit respecter la normativité qui comprend :

- La *Charte des droits et libertés de la personne* (LRQ, chapitre C-12);
- Le *Code civil du Québec* (LQ, 1991, chapitre 64);
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03);
- 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 sur les archives* (LRQ, chapitre A-21.1);
- Le *Code criminel* (LRC, 1985, chapitre C-46);
- Le *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques*;
- La *Politique de gestion des documents inactifs des organismes publics*;

- Le *Règlement relatif à l'utilisation des technologies de l'information* (règlement no. 14 du Cégep);
- La *Directive sur la sécurité de l'information gouvernementale*;
- La *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ 2021, C-25).

3. Définitions

Les termes utilisés dans la présente Politique sont définis ci-après.

Actif informationnel	Ensemble des ressources informationnelles ayant une valeur pour la personne physique ou morale qui en est détentrice, et dont la protection nécessite la mise en place de mesures de sécurité particulières, notamment, 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.
Cégep	Collège d'enseignement général et professionnel Édouard-Montpetit (incluant le Centre sportif) et l'École nationale d'aérotechnique (ÉNA).
Code d'accès	Mécanisme d'identification et d'authentification par un code individuel et un mot de passe ou de ce qui en tient lieu, notamment une carte magnétique ou carte à puce, servant à identifier de façon unique un utilisateur qui utilise un actif informationnel du Cégep.
Confidentialité	Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées.
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 des données qui ne subissent aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

Authenticité	Caractère des données ou des biens dont l'origine, ou, le cas échéant, l'auteur, ainsi que l'intégrité ont été attestés.
Irrévocabilité	Caractère définitif d'une information. Une information irrévocable ne peut pas être effacée et son annulation ou sa modification est documentée.
Logiciel	Ensemble des programmes destinés à effectuer un traitement particulier sur un ordinateur. Le terme logiciel est utilisé pour représenter tous les types de programmes notamment les systèmes d'exploitation.
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 un sinistre majeur.
Technologies de l'information	Regroupent les techniques principalement de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie) qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre de l'information.
Gestion de l'information	Ensemble de fonctions qui sont reliées à l'établissement de la politique et des procédures d'acquisition, d'analyse, de stockage, de conservation, d'utilisation, d'évaluation, de circulation de l'information nécessaire à la bonne marche et au développement du Cégep et sur lesquelles repose la mise sur pied du système informatique de traitement de cette information.
Utilisateur	Toute personne physique ou morale utilisant ou ayant accès aux actifs informationnels du Cégep. Sont considérés comme des utilisateurs les membres du personnel enseignant, les membres du personnel professionnel, les membres du personnel de soutien, les membres du personnel d'encadrement, les hors cadres, les membres de la population étudiante, les personnes retraitées du Cégep et les tiers autorisés (par exemple, des consultants, des fournisseurs, des partenaires).

4. Principes directeurs

4.1. Imputabilité

Le Cégep met à la disposition des utilisateurs des équipements informatiques et logiciels dans le cadre de l'exercice de leurs fonctions reconnues par le Cégep. Ces derniers assument des responsabilités spécifiques quant à l'utilisation de ces outils et sont redevables de leurs actions. Le Cégep Édouard-Montpetit prend les mesures nécessaires pour s'assurer de leur usage adéquat.

4.2. Mesures de sécurité

Le Cégep met en place des mesures de protection, de détection, de prévention et de correction pour assurer la disponibilité, la confidentialité, l'intégrité et l'irrévocabilité de l'actif informationnel de même

que la continuité des activités. Ces mesures préviennent notamment les accidents, l'erreur, la malveillance, l'indiscrétion ou la destruction d'information sans autorisation.

4.2.1 Protection des renseignements personnels

Le droit d'accès aux renseignements personnels des utilisateurs est un pouvoir qui est délégué par la Direction générale et contrôlé par la Direction des systèmes et technologies de l'information (DiSTI). Chaque système prévoit des droits d'accès différents selon les catégories de personnel. Les renseignements personnels ne sont utilisés et ne servent qu'aux fins pour lesquels ils ont été recueillis. Des règles de gouvernance en matière de protection des renseignements personnels sont prévues dans une autre politique.

4.2.2 Sensibilisation

Le Cégep a mis en place un programme formel et continu de sensibilisation sur la sécurité de l'information à l'intention de tous les utilisateurs. Il revient à chaque utilisateur de suivre les formations offertes en cybersécurité. Des campagnes de simulation d'hameçonnage seront effectuées tout au long de l'année afin de tester les réflexes du personnel et des étudiants du Cégep. Des activités de sensibilisation adaptées et personnalisées viendront compléter le programme. Chaque utilisateur doit lire la présente politique, ainsi que les directives de sécurité informatique du Cégep.

4.2.3 Accès aux actifs informationnels du Cégep

Les accès directs aux actifs informationnels sont attribués aux membres du personnel en fonction des contrats d'embauche enregistrés dans le système des ressources humaines. Les accès sont attribués aux membres du personnel administratif et aux membres du corps professoral à la suite de l'émission d'une autorisation formelle provenant de leur supérieur immédiat ou de leur responsable.

Les accès sont attribués aux membres de la population étudiante après la confirmation de leur admission.

L'accès de l'utilisateur aux ressources doit respecter le principe du moindre privilège. Les droits d'accès doivent être revus périodiquement et les utilisateurs doivent être avertis des changements sur ceux-ci.

Les comptes utilisateurs doivent toujours être associés à un utilisateur unique. Les comptes génériques (compte utilisé par plus d'une personne) ne sont pas autorisés.

4.2.4 Continuité des opérations

Pour assurer une continuité des services technologies de l'information en cas de sinistre majeur (incendie, cyberattaque, panne de courant prolongée, inondation, malveillance, etc.), la Direction des systèmes et technologies de l'information a élaboré un Plan de relève informatique qui permet la reprise des activités du Cégep dans un délai raisonnable.

4.3. Directives techniques

Pour accorder les accès des utilisateurs aux données du Cégep, des méthodes de contrôle d'accès doivent être utilisées. Il s'agit :

- De la séparation des réseaux;
- De la protection des données sensibles au repos et en transit;
- Des autorisations sur les fichiers;
- Des accès aux zones réseau;
- De l'audit des tentatives de connexion sur les systèmes du Cégep;
- D'un modèle d'accès basé sur les rôles;
- Des droits d'accès pour certains sites ou applications;
- Des droits d'accès aux serveurs, aux ordinateurs, et à certains locaux;
- Des droits d'accès aux bases de données;
- Des droits d'accès basés sur les principes du besoin de savoir et du moindre privilège.

5. 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 numérique ou ses moyens de communication.

Cette politique vise à assurer le respect de toute législation à l'égard de l'usage et du traitement de l'information et de l'utilisation des technologies de l'information et des télécommunications, pour que toutes les activités pédagogiques et administratives du Cégep se déroulent dans les meilleures conditions possibles.

Plus spécifiquement, voici les objectifs en matière de sécurité de l'information :

- Identifier, réduire et contrôler les risques pouvant porter atteinte aux systèmes d'information du Cégep en favorisant la participation des utilisateurs dans cette démarche de prévention et en réduisant au strict nécessaire l'accès aux données confidentielles et sensibles;
- Assurer la disponibilité, l'intégrité et la confidentialité de l'information durant toute la durée de son cycle de vie;
- Établir un Plan de relève informatique.

Des normes et des procédures viennent appuyer cette politique afin de préciser les règles et obligations qui en découlent et d'assurer sa mise en œuvre.

6. Champs d'application

6.1. Actifs visés

Cette politique s'applique aux actifs informationnels qui appartiennent :

- Au Cégep Édouard Montpetit et qui sont exploités par celui-ci;
- Au Cégep et qui sont exploités par un fournisseur de services ou par un tiers;
- À un fournisseur de services ou à un tiers et qui sont exploités par lui au bénéfice du Cégep Édouard-Montpetit.

Elle s'applique à tous les systèmes informatiques (sur site ou hébergé à l'externe, incluant l'infonuagique) qui traitent les données, y compris tout le matériel informatique ou tout objet connecté qui interagit avec les services informatiques du Cégep.

6.2. Personnes visées

La présente Politique s'adresse aux utilisateurs, tels que définis à l'article 3.

6.3. Informations visées

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 sont concernés.

7. Rôles et responsabilités

La présente Politique et son application relèvent de différents intervenants à qui des responsabilités spécifiques sont attribuées.

7.1. Conseil d'administration

Adopte la politique ainsi que ses mises à jour.

7.2. Direction générale

Valide la Politique ainsi que ses mises à jour et recommande son adoption au conseil d'administration.

7.3. Secrétariat général

- Recommande les bonnes pratiques en matière de production, classement, catégorisation, partage, diffusion et disposition de l'information;
- En collaboration avec les unités administratives, procède au déclassement et disposition de l'information;
- En collaboration avec la DiSTI, contribue à la préservation des actifs informationnels du Cégep.

7.4. Direction des systèmes et technologies de l'information (DiSTI)

- Définit les orientations institutionnelles en matière de sécurité et d'utilisation des technologies de l'information;
- Développe et met en place des directives, procédures et normes touchant l'utilisation et la sécurité des technologies de l'information;
- Accompagne les gestionnaires du Cégep dans la mise en application de la présente Politique;
- Assure la sécurité des technologies de l'information en déployant les mesures nécessaires et appropriées;
- S'assure, au moyen d'ententes contractuelles, que cette politique soit respectée par toute

personne physique ou morale qui ne fait pas partie des membres du personnel ou des membres de la population étudiante du Cégep, mais qui a accès aux actifs informationnels;

- Élabore et met en œuvre le programme de sensibilisation à la sécurité de l'information pour les membres du personnel et les membres de la population étudiante du Cégep en collaboration avec la Direction des communications et la Direction des affaires étudiantes et communautaires;
- Élabore et s'assure du respect d'un code d'éthique pour tous les membres du personnel de la DiSTI;
- Assure la sécurité des services infonuagiques acquis par le Cégep, selon le modèle de responsabilité partagée entendu avec le fournisseur. Il s'agit minimalement de la sécurité des informations et des données, des comptes et des identités, des appareils mobiles et des ordinateurs.

7.4.1 Répondant en matière de sécurité de l'information (RMSI)

- Participe à l'élaboration de la Politique et à ses mises à jour;
- Assure la coordination et la cohérence des actions en matière de sécurité de l'information menées au Cégep;
- S'assure de la contribution du Cégep au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale;
- Représente le Cégep en matière de déclaration des incidents à portée gouvernementale;
- Est le principal interlocuteur en ce qui concerne la sécurité de l'information du Cégep.

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

- Élabore la Politique et ses mises à jour;
- Assiste les directions dans l'évaluation et la gestion des risques à l'égard de la sécurité de l'information;
- Fournit des directives, propose des solutions, coordonne leur mise en place et facilite la conformité en matière de sécurité de l'information;
- Effectue le suivi des observations et des recommandations des vérificateurs en matière de sécurité de l'information;
- Maintient à jour un registre des propriétaires de l'information;
- Participe au réseau d'alerte gouvernemental (CERT/AQ[1]) dont la coordination est assurée par le Centre des services partagés du Québec;
- Est l'interlocuteur officiel du Cégep auprès du CERT/AQ;
- Assure la coordination de l'équipe de gestion des incidents de sécurité du Cégep et du déploiement des stratégies de réaction appropriées;
- Apporte au RMSI le soutien technique nécessaire dans l'exercice de ses responsabilités;
- Contribue à la mise en place du processus de gestion des incidents du Cégep;
- Contribue à la mise en œuvre du processus gouvernemental de gestion des incidents à travers le réseau des Conseillers Organisationnels en Gestion des Incidents (COGI).

[1] Computer Emergency Response Team de l'Administration québécoise

7.5. Direction des ressources humaines

- Vérifie, au besoin, les antécédents des candidates et des candidats à l'embauche et des membres du personnel impliqués dans la sécurité de l'information;
- Intervient auprès des membres du personnel concernés en cas d'atteinte à la sécurité des technologies de l'information, en collaboration avec la DiSTI et les autres intervenantes et intervenants;
- Informe la DiSTI d'une embauche, d'un changement de fonction et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels du Cégep;
- Informe tout nouveau membre du personnel de ses obligations découlant de la présente Politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information.

7.6. Direction des ressources matérielles

- Contrôle les accès physiques aux locaux du Cégep;
- Gère les moyens d'accès physique (clefs, cartes magnétiques, etc.) aux locaux à accès restreint (salles informatiques, entreposage, etc.);
- Met à jour les informations dans la base de données des clés en suivant le mouvement du personnel au sein du Cégep.

7.7. Personnel d'encadrement

- S'assure que les membres du personnel sous sa responsabilité sont au fait de leurs obligations découlant de la présente Politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information;
- Communique à la DiSTI tout problème d'importance en matière de sécurité de l'information.

7.8. Utilisateur

- Prend connaissance de la Politique et y adhère en respectant les normes, directives et procédures en vigueur en matière de sécurité de l'information;
- Utilise les technologies de l'information mises à sa disposition, aux fins auxquelles elles sont destinées et dans le cadre des accès qui lui sont accordés;
- Informe sa ou son responsable, sa professeure ou son professeur ou la DiSTI de toute violation des mesures de sécurité de l'information dont elle ou il pourrait être témoin.

8. Manquement aux règles de la Politique

Le Cégep exige de toute personne physique ou morale qui utilise ses actifs informationnels de se conformer aux dispositions de la présente Politique ainsi qu'aux normes, directives et procédures qui s'y rattachent. Le non-respect de cette obligation est soumis au processus de sanctions et aux mécanismes de recours prévus aux règlements et politiques du Cégep et aux conventions collectives applicables aux membres du personnel.

9. Entrée en vigueur

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

10. Révision et diffusion

La DiSTI procède à l'examen de la Politique et à sa révision en fonction de l'évolution des obligations législatives et réglementaires afin de tenir compte des nouvelles orientations gouvernementales ou de l'évolution des pratiques en sécurité de l'information. Elle est responsable de la diffusion de cette politique après son adoption.