Cégep de Sainte-Foy

POLITIQUE DE SÉCURITÉ DE L'INFORMATION

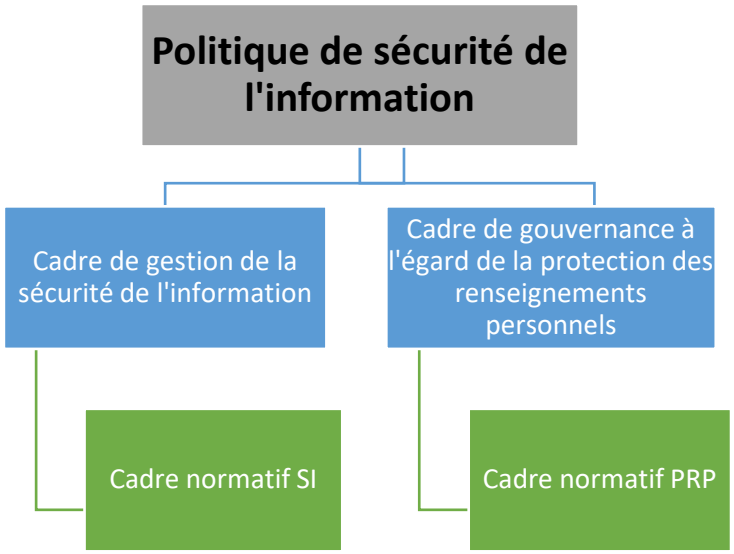
TABLE DES MATIERES

PRÉAMBULE

Le gouvernement du Québec a établi des normes et des obligations en matière de gestion et de protection des informations publiques par le biais de sa *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ c G-1.03 (ci-après appelée la "LGGRI"). Cette loi impose aux organisations la mise en place d'une *Politique de sécurité de l'information* conforme aux normes de l'industrie et aux exigences légales. Parallèlement, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1 (ci-après appelée la "*Loi sur l'accès*"), encadre la gouvernance en matière de renseignements personnels pour les organismes publics.

La *Politique de sécurité de l'information* (ci-après appelée la "*Politique*") propose des principes, des règles, des directives et des processus pour protéger les actifs informationnels, y compris les renseignements personnels, collectés, détenus, utilisés, communiqués et conservés par le Cégep, contre toute perte, tout vol ou toute mauvaise utilisation. Elle vise à garantir la disponibilité, l'intégrité et la confidentialité de l'information et à prévenir les risques. Cette *Politique* complète les lois et règlements qui encadrent les responsabilités du Cégep, notamment en matière de sécurité de l'information et de protection des renseignements personnels, de propriété intellectuelle et de droits d'auteur. Elle guide chaque individu pour qu'il adopte un comportement responsable.

À cette *Politique*, un *Cadre de gestion de la sécurité de l'information* ainsi qu'un *Cadre de gouvernance* à l'égard de la protection des renseignements personnels viennent préciser les obligations qui en découlent. Le graphique ci-dessous montre la relation entre les documents. Les liens d'accès vers les cadres se trouvent en annexe.



1. OBJECTIFS

Les objectifs de la *Politique* sont multiples et ils visent à instaurer une culture de responsabilisation individuelle et organisationnelle en sécurité de l'information au Cégep. La *Politique* vise également à affirmer l'engagement du Cégep de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou son moyen de communication :

- Conscientiser les acteurs clés face à leurs rôles et à leurs obligations en sécurité de l'information, incluant la protection des renseignements personnels ;
- Prévenir les risques en protégeant les informations proportionnellement à leur niveau de sensibilité ;
- Maintenir la disponibilité des informations en s'assurant que les données soient accessibles et utilisables de manière continue et fiable par les entités désignées et autorisées ;
- Assurer l'intégrité des informations pour prévenir toute modification non autorisée des données, afin de garantir leur fiabilité et leur exactitude ;
- Garantir la confidentialité des informations en s'assurant qu'elles ne soient accessibles qu'aux personnes ou entités désignées et autorisées ;
- Répondre aux exigences légales et réglementaires en matière de protection des données, incluant les renseignements personnels et la sécurité de l'information.

2. CHAMPS D'APPLICATION

La *Politique* s'applique à tous les actifs informationnels détenus et utilisés dans le cadre des opérations du Cégep, que les données soient enregistrées ou transmises et quel que soit le support utilisé (papier, électronique, numérique, etc.). Elle couvre également tous les éléments de l'infrastructure (réseaux, systèmes informatiques, bases de données, applications, etc.) qui sont utilisés pour recevoir, stocker, traiter ou transmettre de l'information.

La *Politique* s'adresse aux utilisateurs, c'est-à-dire à toute personne physique ou morale qui, à titre d'employé, d'étudiant, de consultant, de partenaire, de visiteur ou de fournisseur, utilise les actifs informationnels du Cégep ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

Les tiers ayant accès aux renseignements personnels ou à l'information dont le Cégep a la garde ou le contrôle seront informés de la *Politique*, du *Cadre de gestion* et du *Cadre de gouvernance* ainsi que des autres politiques et processus applicables pour assurer la sécurité et la protection des renseignements personnels. Tous les sous-traitants visés devront s'engager par écrit à accepter de se conformer aux politiques, aux processus et aux lois applicables.

3. DÉFINITIONS

Actif informationnel1 : 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 ou utilisable avec un dispositif technologique (logiciel, progiciel, didacticiel, banque 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.

Authentification : Est une procédure permettant pour un système informatique de vérifier l'identité d'une personne ou d'un ordinateur et d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications).

Base de données : est une collection organisée d'informations structurées, généralement stockées électroniquement dans un système informatique.

Cégep : Collège d'enseignement général et professionnel de Sainte-Foy.

Confidentialité : Propriété que possède une information ou une donnée de n'être accessible qu'aux personnes ou entités désignées et autorisées.

Disponibilité : Propriété que possède une information ou une donnée d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Intégrité : Propriété des données ou informations qui ne subissent aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

ISO : La norme ISO 27000 (officiellement connue sous le nom de ISO/IEC 27000) est une norme internationale qui établit les exigences pour un système de gestion de la sécurité de l'information (SMSI). La norme ISO 27000 fournit un cadre pour la mise en place, la mise en œuvre, la maintenance et l'amélioration continue de la sécurité de l'information au sein d'une organisation.

L'infonuagique : est un modèle d'accès au réseau habilitant, pratique et sur demande comprenant un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peut rapidement être activé et désactivé en réduisant au minimum les efforts de gestion ou les contacts avec le fournisseur de services.

[1] Tout document dont la définition correspond à celle de l'article 3 et 4 de la *Loi concernant le cadre juridique des technologies de l'information* (chapitre C-1.1).

Mitre : est un cadre normatif permettant de partager des renseignements sur les menaces, en fournissant un langage commun et normalisé, universel et facile d'accès. https://attack.mitre.org/

NIST : Institut National des Standards et Technologies est un cadre utilisé pour renforcer la position de cybersécurité et comporte un processus en cinq étapes pour gérer les risques de cybersécurité et maintenir l'infrastructure de sécurité à l'aide de mesures d'identification, de protection, de détection, de réponse et de rétablissement après une attaque. https://www.nist.gov/cyberframework

Renseignement personnel: Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent directement ou indirectement de l'identifier, tels que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la photographie et les coordonnées bancaires. Les renseignements personnels sont confidentiels sauf dans les cas prévus à la *Loi sur l'accès*. Les renseignements personnels doivent être protégés, peu importe la nature de leur support et quelle que soit leur forme : écrite, graphique, sonore, visuelle, informatisée ou autre.

Sécurité de l'information : La protection de l'information et des systèmes d'information contre les risques.

Système informatique : un système automatisé de stockage, de traitement et de récupération de données qui tire parti des outils informatiques et électroniques pour effectuer une série complexe de processus et d'opérations.

Utilisateur : Toute personne physique ou morale qui utilise les actifs informationnels sous la responsabilité du Cégep.

4. CADRE JURIDIQUE ET ADMINISTRATIF

La *Politique* s'inscrit notamment dans un contexte régi par les lois suivantes et les règlements pris en vertu de ces lois :

- La *Charte des droits et libertés de la personne*, RLRQ c C-12;
- Le *Code civil du Québec*, RLRQ c CCQ-1991;
- La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ c G-1.03;
- La *Loi concernant le cadre juridique des technologies et l'information*, RLRQ c C-1.1;
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1;
- La *Loi sur les archives*, RLRQ c A-21.1;
- La *Loi sur l'administration publique*, RLRQ c A-6.01;

- La *Loi sur la fonction publique*, RLRQ c F-3.1.1;
- La Loi canadienne sur les droits de la personne, LRC 1985, c H-6;
- Le *Code criminel*, LRC 1985, c C-46;
- La *Loi sur le droit d'auteur*, LRC 1985, c C-42;
- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, RLRQ c A-2.1, r 2;
- La *Directive sur la sécurité de l'information gouvernementale* (Secrétariat du Conseil du Trésor, récemment remplacé par le ministère de la Cybersécurité et du Numérique).

5. PRINCIPES DIRECTEURS

Les principes suivants guident la démarche du Cégep afin de régir le fonctionnement, l'organisation et la gestion de la sécurité de l'information :

Conformité gouvernementale, légale et réglementaire

Structurer la gestion de la sécurité de l'information et la gouvernance à l'égard de la protection des renseignements personnels et confidentiels, en conformité aux orientations et objectifs gouvernementaux, légaux et réglementaires.

Utilisation des meilleures pratiques

S'engager à ce que les pratiques et les solutions retenues correspondent, dans la mesure du possible, aux meilleures pratiques en matière de sécurité de l'information, notamment les normes ISO-27000, NIST ou Mitre.

Mise en œuvre d'un cadre normatif

Mettre en œuvre un cadre normatif en sécurité de l'information constitué de mesures de protection, de détection, de prévention et de correction pour assurer la disponibilité, l'intégrité, la confidentialité, l'authentification et l'irrévocabilité ainsi que la continuité des services.

Responsabilisation de l'utilisateur

Appuyer les mesures de sécurité de l'information sur la responsabilité individuelle, en misant sur la sensibilisation et la formation des utilisateurs à la sécurité des actifs informationnels et la protection des renseignements personnels, aux conséquences d'une atteinte à leur sécurité et à leur confidentialité ainsi qu'à leur rôle et à leurs obligations en la matière.

Droit de regard et d'intervention

Le Cégep exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard et d'intervention sur ses actifs informationnels afin d'assurer le respect de son cadre normatif.

6. RÔLES ET OBLIGATIONS

Obligations des intervenants clés en matière de sécurité de l'information et de protection des renseignements personnels

Les rôles et obligations des intervenants clés en matière de sécurité de l'information dépendent du contexte dans lequel ils exercent leurs activités et de la nature des informations qu'ils gèrent. Ils sont définis dans le *Cadre de gestion de la sécurité de l'information* et dans le *Cadre de gouvernance* à l'égard de la protection des renseignements personnels, complémentaires à la *Politique*.

Il est de la responsabilité de chaque intervenant de lire et connaître les obligations découlant des cadres précités.

Chaque intervenant s'engage à respecter la *Politique* en signant la déclaration d'engagement jointe en annexe.

La présente *Politique* fixe en matière de sécurité de l'information et de protection des renseignements personnels, selon le cas, les obligations attribuées, notamment à la Direction générale, au chef de la sécurité de l'information organisationnelle (CSIO), aux coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI), au responsable de l'accès à l'information et de la protection des renseignements personnels et aux répondants en matière de sécurité de l'information.

6.1 LA DIRECTION GÉNÉRALE

Le dirigeant d'un établissement du réseau de l'éducation est le premier responsable de l'information relevant de son autorité. Il est également le responsable de l'application des lois qui définissent le cadre juridique de la gestion de l'information.

6.2 LE CHEF DE LA SÉCURITÉ DE L'INFORMATION ORGANISATIONNELLE (CSIO)

Le CSIO assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein du Cégep. 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.

6.3 LES COORDONNATEURS ORGANISATIONNELS DES MESURES DE SÉCURITÉ DE L'INFORMATION (COMSI)

Le COMSI représente le Cégep auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) au Cégep, en soutien à son chef de la sécurité de l'information organisationnelle (CSIO).

6.4 RESPONSABLE DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Cette personne veille à assurer la mise en œuvre de la *Loi sur l'accès* lorsque cette fonction lui est déléguée par la Direction générale.

6.5 RÉPONDANTS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

Toute personne physique ou morale qui utilise les actifs informationnels sous la responsabilité du Cégep participe aux activités relatives à la sécurité de l'information et à la protection des renseignements personnels, en fonction des rôles et responsabilités respectifs. La liste des personnes responsables de la sécurité comprend, notamment les gestionnaires, les détenteurs d'information et les utilisateurs.

7. MANQUEMENT À LA POLITIQUE

Tout utilisateur qui contrevient à la *Politique*, ainsi qu'aux mesures de sécurité de l'information et de protection des renseignements personnels qui en découlent ou au cadre légal sur laquelle elle s'appuie, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi et des règles disciplinaires internes applicables. Les sanctions que le Cégep peut appliquer peuvent prendre différentes formes, notamment la réprimande, l'expulsion, la suspension, le renvoi ou toute autre sanction prévue aux lois et aux règlements ou d'autres mesures selon la nature des manquements associés aux politiques, règlements ou directives du Cégep ainsi qu'aux conventions collectives.

Toute contravention à la *Politique*, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au Cégep ou en vertu des dispositions de la législation et de la réglementation applicable en la matière.

8. ENTRÉE EN VIGUEUR ET RÉVISION

La *Politique* et ses amendements ultérieurs entreront en vigueur dès leur adoption par le conseil d'administration.

L'examen et la révision de la *Politique* se réalisent lorsque l'évolution du cadre juridique ou social l'exige ou au plus tard 5 ans après son adoption et à tous les 5 ans par la suite.

Adoptée par le conseil d'administration le 15 mai 2023, cette Politique remplace celle nommée Politique sur la sécurité de l'information qui avait été adoptée le 23 avril 2018.

ANNEXE 1

DÉCLARATION D'ENGAGEMENT PAR LES UTILISATEURS QUANT AU RESPECT DES RÈGLES DE SÉCURITÉ DE L'INFORMATION, DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE CONFIDENTIALITÉ

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition par le Cégep de Sainte-Foy. À cette fin, ils doivent :

- Se conformer à la *Politique sur la sécurité de l'information*, au *Cadre de gestion de la sécurité de l'information*, au *Cadre de gouvernance* à l'égard de la protection des renseignements personnels ainsi qu'aux directives, aux procédures et aux autres lignes de conduite se rapportant à la sécurité de l'information du Cégep et à la protection des renseignements personnels.
- Utiliser, dans le cadre des droits d'accès qui leur sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels mis à leur disposition, en se limitant aux fins auxquelles ils sont destinés.
- Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier la configuration des mesures de sécurité ou les désactiver.
- Se conformer aux règles relatives à la gestion documentaire, à la confidentialité et à la conservation des actifs informationnels.
- 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 leur supérieur tout acte dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité et de confidentialité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du Cégep.
- Au moment de leur départ du Cégep, remettre les différents moyens d'accès (exemples : cartes et clés), les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de l'exercice de leurs fonctions.

Je soussigné(e), _____, reconnais avoir pris connaissance des règles, ci-dessus reproduites, sur la sécurité de l'information du Cégep de Sainte-Foy et m'engage à les respecter.

Signature : _____ Date : _____

ANNEXE 2

LIENS

Cadre de gestion de la sécurité de l'information

Cadre de gouvernance à l'égard de la protection des renseignements personnels