Règlements, politiques, procédures et directives

Service : **DTIRI**
Numéro de sujet : **001**

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Adoptée au CA le 25 avril 2023

1. PRÉAMBULE

Le Cégep de St-Félicien et l'ensemble de ses constituantes (le Centre d'études collégiales à Chibougamau, le Service aux entreprises et aux collectivités et le Centre de transfert technologique Écofaune boréale) reconnaissent l'influence et l'importance grandissante des technologies de l'information et des communications (TIC) en soutien à l'apprentissage et comme moteur de réussite éducative.

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 St-Félicien 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, d'information professionnelle sujette à des droits de propriété intellectuelle et d'information stratégique ou opérationnelle 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.

2. DÉFINITIONS

Actif informationnel : Tout système ou équipement du Cégep, pouvant être sa propriété ou loués permettant le traitement, le transport et l'entreposage de toute forme de communication ou d'information, notamment les équipements informatiques (postes de travail, ordinateurs portables, imprimantes, etc.), les réseaux de communication (Internet, réseau local, réseau sans-fil, réseau étendu, etc.), les services en ligne, les systèmes de téléphonie, les systèmes de vidéosurveillance et de télécommunication, le courrier électronique, les bases de données, les images numérisées, les vidéos, les applications et les progiciels ainsi que la documentation nécessaire à leur bon fonctionnement.

Autorisation - Droit d'accès : L'attribution par le Cégep à une personne ou à un groupe de personnes d'un droit d'accès, complet ou restreint, à une information ou à un système d'information.

COMSI : Coordonnateur organisationnel des mesures de sécurité de l'information. Rôle exigé par le cadre gouvernemental de gestion de la sécurité de l'information du Québec. Ce rôle sera assumé par le directeur des technologies de l'information et des ressources informationnelles.

Cycle de vie de l'information : L'ensemble des étapes que franchit une information, de sa création en passant par sa sauvegarde, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation du Cégep.

Direction des technologies de l'information et des ressources informationnelles (DTIRI) : Regroupe l'ensemble du personnel professionnel et technique sous l'autorité de la directrice ou du directeur de la DTIRI.

Information : Un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Intégrité des données : Propriété d'une information qui n'a subi aucune altération ni destruction sans autorisation et conservée sur un support numérique et préservé par des moyens lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude des données.

Nétiquette : L'ensemble des conventions de bienséance qui régissent le comportement des internautes dans le réseau Internet, notamment lors d'échanges dans les forums, par courriel et dans les médias sociaux. La nétiquette fait référence à des règles de politesse et de savoir-vivre que doivent appliquer les utilisatrices et les utilisateurs des TI. On retrouve la nétiquette à l'annexe 1.

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

Renseignement confidentiel : Un renseignement dont l'accès est assorti d'une ou de plusieurs restrictions, dont celles prévues principalement par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Renseignement personnel : Un renseignement personnel est une information portent sur une personne physique et permettent de l'identifier.

Responsable d'actifs informationnels : Membre du personnel d'encadrement détenant la plus haute autorité au sein d'une unité pédagogique ou administrative 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 unité.

Ressource informationnelle : Une ressource informationnelle est une ressource utilisée par une entreprise ou une organisation, dans le cadre de ses activités de traitement de l'information, pour mener à bien sa mission, pour faciliter la prise de décision ou encore la résolution de problèmes. Une ressource informationnelle peut être une ressource humaine, matérielle ou financière directement affectée à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à la destruction des éléments d'information. Une ressource peut donc être une personne, un fichier ou le système informatique lui-même.

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 à une atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et pouvant avoir des conséquences sur la prestation des services, la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux, la protection de leurs renseignements personnels et le respect de leur vie privée ou sur la réputation du Cégep.

Chef de la sécurité de l'information organisationnelle (CSIO): Rôle exigé par le cadre gouvernemental de gestion de la sécurité de l'information du Québec. Le directeur des technologies de l'information et des ressources informationnelles est le responsable.

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

Système d'information : L'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, incluant notamment les applications, progiciels, logiciels, technologies de l'information et procédés utilisés pour accomplir ces fonctions.

Support numérique : Support de stockage sur lequel sont conservées des informations sous forme numérique.

3. CADRE LÉGAL ET ADMINISTRATIF

Le Cégep en sa qualité d'organisme public est soumis à plusieurs directives, lois ou règlements émis par le gouvernement du Québec.

Ainsi, cette Politique s'inscrit principalement dans un contexte régi par les lois et documents suivants :

- la Charte des droits et libertés de la personne (LRQ, chapitre C-12),
- le Code civil du Québec (LQ, 1991, chapitre 64),
- 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 (LGGRI) (LRQ, chapitre G-1.03, amendé en 2017),
- la Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1),
- la Politique gouvernementale de cybersécurité (SCT, 2020),
- 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),
- la Loi sur l'administration publique (LRQ, chapitre A-6.01),
- la Loi sur la fonction publique (LRQ, chapitre F-3.1.1),
- la Loi canadienne sur les droits de la personne (LRC, 1985, chapitre H-6),
- le Code criminel (LRC, 1985, chapitre C-46),
- la Loi sur le droit d'auteur (LRC, 1985, chapitre C-42),
- le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 02),
- la Directive sur la sécurité de l'information gouvernementale (DSIG),
- l'architecture stratégique gouvernementale de la sécurité de l'information (ASGI),
- la certification ISO 27001 – Sécurité de l'information,
- les politiques et règlements du Cégep.

4. OBJECTIFS DE LA POLITIQUE

La présente politique a principalement pour objectif d'affirmer l'engagement du Cégep de St-Félicien à 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 par le Cégep,
- 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 de cette information lui procure la stabilité et la pérennité voulues,
- la **confidentialité** de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels ou sensibles,
- définir les **obligations et les responsabilités** des membres de la communauté collégiale en lien avec la sécurité de l'information.

5. CHAMP D'APPLICATION

La présente politique s'adresse à tous les utilisateurs, c'est-à-dire à toute personne physique ou morale qui, à titre d'employé(e), d'étudiant(e), de consultant(e), de partenaire, de fournisseur, d'invité(e) ou toute personne dûment autorisée par le Cégep, qui utilise ou accède les ressources informationnelles externes ou internes du Cégep. Cette politique vise l'entièreté de l'information détenue par le Cégep dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou un tiers, et ce, sans regard au type de support qui la contient.

6. PRINCIPES DIRECTEURS

6.1 Utilisation de l'information

Le Cégep reconnaît que ses actifs informationnels soutiennent ses activités professionnelles et pédagogiques et que les utilisatrices et utilisateurs en font usage à ces fins. Le Cégep s'engage à maintenir un équilibre entre l'accès aux outils permettant la prestation de travail et le niveau des mesures de sécurité appliquées à ses actifs informationnels.

Le Cégep s'engage à mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels à tous ses utilisateurs, selon un temps prévu dans le but de réduire au minimum les risques représentés par une situation d'urgence.

6.2 Protection de l'information

Le Cégep de St-Félicien 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 niveau de confidentialité ainsi que 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 ; chaque individu qui a accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci.

6.3 Engagement des utilisateurs

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

6.4 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 les 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.

6.5 Sensibilisation et formation

Le Cégep s'engage, sur une base régulière, à sensibiliser et à former 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.

6.6 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.

7. CADRE DE GESTION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents acteurs du Cégep par la mise en place d'un cadre de gestion de la sécurité permettant notamment 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 dans le but 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.

7.1 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 but 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 et une imputabilité de tous les membres du personnel et sur l'obligation pour chaque membre d'en rendre compte selon leur fonction au sein du Cégep.

7.2 Gestion des risques

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

L'analyse de risques guide également l'acquisition, le développement 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 par le Cégep.

7.3 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, le Collège met en place de façon proactive les mesures suivantes :

- Rechercher, corriger et réduire les vulnérabilités de l'organisation face aux menaces en matière de sécurité de l'information en appliquant les bonnes pratiques en cette matière,
- Gérer adéquatement les incidents afin de minimiser les conséquences et rétablir les activités et les opérations,
- Mettre en place des mesures correctives lors d'un incident afin de rétablir les services affectés et éviter les impacts sur les utilisatrices et utilisateurs,
- Déclarer les incidents de sécurité de l'information à portée gouvernementale au Centre opérationnel en cyberdéfense (COCD) du ministère de l'Enseignement supérieur conformément à la DSIG et à la Politique gouvernementale en cybersécurité,
- Exercer ses pouvoirs et ses prérogatives à l'égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

8. OBLIGATIONS ET RESPONSABILITÉS DES INTERVENANTS CLÉS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents responsables du Cégep. 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 de sécurité de l'information ainsi que toute mise à jour de celle-ci. Le conseil est informé des actions du Cégep en matière de sécurité de l'information lors du dépôt du rapport d'activités annuel du collège ou immédiatement lors d'incident majeur de sécurité informationnel. Le directeur général est le dirigeant de l'organisme responsable de l'application de la politique en sécurité de l'information.

Le comité exécutif du conseil d'administration peut également prendre des décisions relativement à la présente politique dans un cadre déterminé au préalable par ce dernier.

8.2 Comité de régie administrative

Le comité de régie administrative 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 détermine les orientations stratégiques, les plans d'action et les bilans de sécurité de l'information. Il peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

8.3 Direction générale

La direction générale veille à l'application de la politique sur la sécurité de l'information. Elle a pour responsabilité :

- de soutenir la direction des technologies de l'information et des ressources informationnelles dans la réalisation de son mandat de sécurité de l'information,
- de faire adopter, s'il y a lieu, par le conseil d'administration les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information,
- d'autoriser une enquête lors d'une transgression de la politique.

8.4 Direction des technologies de l'information et des ressources informationnelles (DTIRI)

Le directeur de la DTIRI assume les responsabilités du **CSIO et de COMSI**. Relevant de la direction générale, il met en place le cadre de gestion de la sécurité de l'information et s'assure que les objectifs et moyens mis en place répondent aux besoins en matière de sécurité de l'information.

Cette personne:

- élabore et propose le programme de sécurité de l'information du Cégep, rend compte de son implantation au comité de régie administrative,

- 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. De plus, il est responsable de mettre à jour la politique,
- 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,
- produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information,
- 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,
- s'assure de la déclaration par le Cégep des risques et des incidents de sécurité de l'information qui ont une portée gouvernementale (CERT/AQ),
- 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,
- procède aux enquêtes dans des transgressions présumées et sérieuses ayant trait à la politique, à la suite de l'autorisation du dirigeant de l'organisme,
- 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,
- met en place un plan de continuité des services en cas d'incident de sécurité de l'information (feu, dommage causé par l'eau, cyberattaque, etc.) portant atteinte aux actifs informationnels,
- 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 actifs informationnels,
- applique des mesures préventives et de réaction appropriée à toute menace ou à tout incident de sécurité de l'information,
- participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la direction générale,
- collabore à la production d'outils de communication visant à sensibiliser et à former les utilisatrices et les utilisateurs.

8.5 Direction des services administratifs - ressources matérielles

Le responsable des ressources matérielles au sein de la direction des services administratifs (DSA) participe, avec le responsable de la sécurité de l'information, à l'identification des mesures de sécurité physiques permettant de protéger adéquatement les actifs informationnels du Cégep.

8.6 Direction des ressources humaines

La direction des ressources humaines (DRH) s'assure de communiquer régulièrement les mouvements de personnel à la DTIRI afin de s'assurer que les utilisatrices et les utilisateurs se voient octroyer les droits d'accès appropriés.

Elle transmet périodiquement à la DTIRI des listes de membres du personnel actifs, retraités ou ayant quitté le Cégep pour permettre la validation de la liste des comptes utilisateurs attribués, leur activation ou leur désactivation, ainsi que la récupération de leurs équipements technologiques.

La DRH est aussi responsable de faire connaître à chaque nouvel employé cette présente politique et les obligations qui en découlent.

Elle intervient dans les cas de non-respect de la présente politique par un ou des membres du personnel et dans l'établissement des sanctions appropriées.

8.7 Responsable d'actifs informationnels

Le responsable d'actifs informationnels est le cadre 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. Il peut donc y avoir plusieurs responsables d'actifs informationnels dans un Cégep. Le 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 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 consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion,
- rapporte au service informatique 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 au directeur de la DTIRI 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.

8.8 Responsable de la gestion documentaire

Le responsable de la gestion documentaire relève de la direction générale. Il a comme responsabilité la gestion des documents du Cégep.

Cette personne :

- collabore au pilotage des systèmes informatiques, administratifs ou autres et s'assure qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires afin de se conformer aux bonnes pratiques en matière de sécurité informationnelle,

- collabore étroitement avec les responsables d'actifs informationnels, en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

8.9 Responsable de l'accès à l'information

La personne responsable de l'accès à l'information veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1)* par le Collège. Elle s'assure du respect de la présente politique dans l'exercice de ses fonctions. La directrice ou le directeur général est le responsable.

8.10 Responsable de la protection des renseignements personnels

La personne responsable de la protection des renseignements personnels veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1)* par le Collège. Elle s'assure du respect de la présente politique en matière de protection des renseignements personnels. La directrice ou le directeur général est le responsable sauf si cette responsabilité est déléguée à une autre personne.

8.11 Utilisateurs

Le respect de la présente politique 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,
- utiliser les actifs informationnels qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés,
- signaler au responsable des actifs informationnels de son unité tout incident susceptible de constituer une contravention à la présente politique ou une menace à la sécurité informationnelle du Cégep,
- collaborer à toute intervention visant à indiquer ou à circonscrire une menace à la sécurité de l'information ou un incident de sécurité de l'information,
- préserver les actifs informationnels et ne pas modifier leur configuration,
- respecter les mesures en place ainsi que la nétiquette,
- utiliser les actifs informationnels de façon à assurer leur sécurité, leur pérennité et leur durabilité,
- prendre connaissance des informations et des obligations du Cégep concernant la sécurité et l'utilisation des technologies de l'information.

9. SANCTIONS

En cas de contravention à la présente politique, l'utilisateur 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.

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité des ressources informationnelles qui en découlent ainsi que de l'utilisation de tout matériel qui est mis à sa disposition, 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 de travail et des règlements ou politiques internes du Cégep).

De même, 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 applicable en la matière.

10. DIFFUSION ET RÉVISION DE LA POLITIQUE

Le conseil d'administration adopte la politique et assure sa révision au besoin.
La direction générale s'assure du respect de la politique et répond de celle-ci devant le conseil d'administration et recommande, s'il y a lieu, toute modification.
La DTIRI voit à l'application et au respect de la politique et fournit l'assistance nécessaire aux gestionnaires pour l'application de cette politique. Elle est responsable de la promotion, de la révision et de l'évaluation de ladite politique.

11. ENTREE EN VIGUEUR

La présente politique entre en vigueur au moment de son adoption par le Conseil d'administration du Collège.

RÉFÉRENCES

- Cégep de Sherbrooke - Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information, 21 mars 2019.
- Cégep de L'Outaouais – Politique relative à la sécurité de l'information, 15 février 2022
- Cégep de Saint-Jean-Sur-Richelieu – Politique de sécurité de l'information, 20 septembre 2022.
- Cégep de Lanaudière – Nétiquette (https://www.cegep-lanaudiere.qc.ca/netiquette), 2022.
- Cégep de Granby – Nétiquette et bonnes pratiques dans l'univers du virtuel!, janvier 2021.
- Québec – Secrétariat du Conseil du Trésor – Cadre normatif de gestion des ressources informationnelles (https://www.tresor.gouv.qc.ca/ressources-informationnelles/cadre-normatif-de-gestion-des-ressources-informationnelles/#:~:text=Une%20ressource%20informationnelle%20est%20une,encore%20la%20r%C3%A9solution%20de%20probl%C3%A8mes.), 2022.

ANNEXE 1 – La nétiquette

La nétiquette du Cégep de St-Félicien s'adresse aux membres de la communauté collégiale, le personnel et les étudiants, lorsqu'ils interviennent sur les différentes plateformes Teams et Zoom du Cégep, ses espaces dédiés dans les médias sociaux ou encore lors d'échanges par courrier électronique. S'exprimer sur ces différentes plateformes exige courtoisie, politesse, respect des autres et respect de la langue.

Ne sont pas tolérés (exemples) :

1. Les propos haineux, racistes, xénophobes, sexistes ou disgracieux envers l'origine ethnique, l'appartenance à une religion ou à un groupe d'âge.
2. Le langage vulgaire, obscène ou malveillant.
3. Les injures, les insultes, les attaques personnelles, les menaces ou le harcèlement d'une personne.
4. Les propos diffamatoires.
5. Le contenu plagié ou contrevenant aux droits d'auteur, de marque de commerce, etc.
6. Les messages envoyés à répétition, les chaînes de lettres et les pourriels (Spam, promotion, publicité).

Sont à éviter (exemples) :

1. Les messages en majuscules, car les majuscules équivalent aux cris et elles peuvent être interprétées comme de l'agressivité.
2. Les messages sans rapport avec le sujet.
3. Les échanges sous forme de dialogue dans les lieux d'échanges publics (blogues, forums, etc.).

Sont à encourager (exemples) :

1. Le respect de la vie privée des autres.
2. Le respect de votre interlocuteur ou interlocutrice.
3. La préoccupation pour le français : respect de l'orthographe et de la grammaire. Des outils comme Antidote ou Word-Q sont utiles pour corriger un texte ou un message.
4. La participation à la vie numérique et aux interactions sociales pour s'informer et partager.
5. Faire rayonner la mission et les messages du Cégep.

Bonnes pratiques

Lorsque vous êtes sur Internet et que vous utilisez les réseaux sociaux, vous êtes en public. Voici quelques recommandations pour protéger votre réputation et celle du Cégep :

- Si vous avez un doute, ne publiez pas.
- Limitez-vous à votre domaine d'expertise.
- Citez vos sources, le cas échéant.
- Gardez des traces de vos interactions en ligne.