Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information

19.03.20.05

Préambule

Le Cégep de Sherbrooke reconnaît l'influence grandissante du numérique, la nécessité de son intégration aux processus de travail et de gestion de même que son importance pour la formation, le soutien à l'apprentissage et la réussite.

Le Cégep considère essentiel d'encadrer l'utilisation des technologies et de protéger les ressources informationnelles ainsi que les données qui y sont contenues, ceci afin de réduire les risques qui menacent l'intégrité de ses infrastructures, de ses données et de ses applications, puis de se conformer aux lois en vigueur.

La présente Politique confirme l'engagement du Cégep à s'acquitter de ses obligations à l'égard de la sécurité et promeut une utilisation responsable des technologies de l'information (TI).

Objectifs

- Fournir un cadre de référence déterminant les conditions d'utilisation des TI et les mesures de protection des ressources informationnelles.
- S'assurer de maintenir un niveau adéquat de disponibilité, d'intégrité et de confidentialité de l'information selon les besoins.
- Définir les rôles et les responsabilités des membres de la communauté collégiale.

Cadre juridique

La présente Politique s'inscrit dans un contexte régi par plusieurs lois, obligations et principes de gestion généralement reconnus dans le domaine, notamment :

- 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);
- 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);
- 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;
- le référentiel de bonnes pratiques d'audit informatique et de gouvernance des systèmes d'information (COBIT : Control Objectives for Information and related Technology).

Champs d'application

Cette politique s'adresse aux personnes utilisant les actifs informationnels du Cégep, c'est-à-dire à tous les membres du personnel et de la population étudiante, aux partenaires, aux fournisseurs ainsi qu'aux personnes et organismes utilisant les services du Cégep.

L'information visée est celle utilisée par le Cégep dans le cadre de ses activités, que sa conservation en soit assurée par le Cégep ou par un tiers.

Article 1 – Définitions

Actif informationnel : Tout système ou équipement du Cégep, pouvant être sa propriété ou loué, 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.

Cadre de gestion : L'ensemble des directives, des procédures et des bonnes pratiques reconnues qui encadrent les activités du Cégep en lien avec l'utilisation et la sécurité des TI,
de même que les attentes à l'égard des utilisatrices et des utilisateurs.

COGI : Le coordonnateur organisationnel de gestion des incidents. Rôle exigé par le cadre gouvernemental de gestion de la sécurité de l'information du Québec.

Cycle de vie de l'information : L'ensemble des étapes que franchit une information, de sa création en passant par son enregistrement, 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.

Incident : Un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information.

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

Intégrité des données : La propriété d'une information de ne subir aucune altération ni destruction sans autorisation et d'être conservée sur un support et préservée par des moyens lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude des données.

Néthique : L'ensemble des principes moraux qui régissent le comportement des internautes dans le réseau Internet. Elle comprend les règles de conduite à caractère moral. On retrouve la néthique en annexe à la Politique des communications.

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 en annexe de la Politique des communications.

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.

Responsable de logiciel institutionnel : Un membre du personnel-cadre responsable du fonctionnement d'un logiciel administratif ou pédagogique identifié comme étant nécessaire à la réalisation de la mission du Cégep.

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.

RSI : Responsable de la sécurité de l'information dont le rôle est exigé par le cadre gouvernemental de gestion de la sécurité de l'information du Québec.

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.

Technologie de l'information (TI) : Tout logiciel ou matériel électronique ou toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme.

Utilisateur ou utilisatrice : Toute personne autorisée par le Cégep à utiliser ses services et ses actifs informationnels, soit les membres de la communauté collégiale de même que les fournisseurs et les partenaires internes.

Article 2 – Principes directeurs – Utilisation des technologies de l'information

a) Seules les personnes autorisées ont le droit d'utiliser les actifs informationnels du Cégep.

b) Le Service des technologies de l'information (STI) est l'unique service autorisé à gérer et à distribuer les droits d'utilisation.

c) Les actifs informationnels du Cégep doivent être utilisés à des fins reliées aux activités de l'établissement, à moins qu'il en soit explicitement convenu autrement entre les parties. L'utilisation des actifs de l'établissement à des fins commerciales autres que celles du Cégep est interdite, tout comme l'utilisation de ses équipements en vue du stockage de données commerciales qui ne sont pas en lien avec ses activités. Il est également interdit d'utiliser, à des fins commerciales personnelles, les licences de logiciels et d'équipements spécialisés qui sont sous la propriété du Cégep.

d) Il est interdit d'utiliser les actifs informationnels à des fins de consultation ou de propagande de nature violente, sexiste, raciste, haineuse, homophobe ou pornographique.

e) Le STI est responsable de gérer, configurer, acquérir, réparer, déplacer, prêter et retirer des actifs informationnels ainsi qu'à établir les conventions de prêt pour les équipements mobiles. Des dérogations pourraient toutefois être obtenues sur demande après du STI pour la gestion et la configuration d'équipements. Nul ne peut modifier ou utiliser les actifs informationnels pour causer des pannes ou bloquer des accès.

f) L'utilisatrice ou l'utilisateur est responsable en tout temps de gérer, de protéger et de conserver confidentiellement ses codes d'accès et ses mots de passe. En tout temps, elle ou il est responsable des actions effectuées à l'aide de ceux-ci.

g) Si la gravité de la situation le justifie, la direction générale autorise le responsable du STI à utiliser des moyens de surveillance des activités réalisées en lien avec les ressources informationnelles, et ce, dans le but de protéger les actifs informationnels de même que les utilisatrices et utilisateurs.

Article 3 – Principes directeurs – Sécurité des technologies de l'information

Le Cégep :

a) reconnaît l'importance de la sécurité de l'information et du cadre de gestion qui la concerne;

b) reconnaît que l'environnement technologique est en changement constant et interconnecté avec le monde et met en place une gestion de la sécurité de l'information qui s'adapte à ces changements;

c) protège les actifs informationnels tout au long de leur cycle de vie, c'est-à-dire de leur acquisition ou création jusqu'à leur destruction;

d) s'assure de bien connaître l'information à protéger et ses caractéristiques de sécurité et de maintenir à jour l'inventaire des actifs informationnels;

e) adhère à une approche basée sur la gestion des risques et reconnaît l'importance d'évaluer régulièrement ces risques;

f) s'assure de mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information;

g) définit des actions pour éradiquer les menaces ou recouvrer les actifs informationnels compromis;

h) adhère à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle;

i) veille à ce que chaque utilisateur et utilisatrice ait accès à l'information requise pour accomplir ses tâches;

j) communique de façon transparente au sujet des menaces pouvant affecter les actifs informationnels, et ce, afin que les utilisatrices et les utilisateurs puissent comprendre l'importance d'appliquer les mesures de sécurité, soient en mesure de reconnaître les incidents de sécurité et qu'ils y réagissent adéquatement.

k) s'assure de mettre en place un plan de continuité des activités en vue de rétablir les services essentiels à sa mission.

Article 4 – Cadre de gestion

Cette politique est complétée par un cadre de gestion de la sécurité et de l'utilisation des TI venant préciser les directives, les procédures, les bonnes pratiques de même que les attentes à l'égard des utilisatrices et des utilisateurs.

Article 5 – Rôles et responsabilités

La présente Politique attribue la gestion de la sécurité de l'information du Cégep à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

5.1 Conseil d'administration

Le conseil d'administration est responsable de l'adoption de la présente Politique et de son actualisation. Il adopte les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité et les redditions de comptes en matière de sécurité de l'information prévues à la règlementation. Il doit ainsi être régulièrement informé des actions menées au Cégep en matière de sécurité et d'évolution des TI.

5.2 Conseil de régie

Le conseil de régie du Cégep, auquel participent tous les directeurs et directrices de même que la personne à la coordination du STI, détermine des mesures favorisant l'application de la Politique. Il détermine les orientations stratégiques, les plans d'action et approuve les bilans de sécurité de l'information. Il est consulté lors de l'élaboration et de la modification du cadre de gestion de la Politique. Le conseil de régie agit également à titre de cellule d'urgence lors d'incidents de sécurité importants.

5.3 Direction générale

La direction générale veille à l'application de la présente Politique. Elle a pour responsabilité :

a) de soutenir le RSI dans la réalisation de son mandat;

b) de faire adopter par le conseil d'administration les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité et les redditions de comptes en matière de sécurité de l'information prévues à la règlementation;

c) d'autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente Politique, à une directive ou une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission du Cégep;

d) d'autoriser une enquête lorsqu'il y a ou pourrait y avoir manquement à la Politique ou un risque pour la sécurité des ressources informationnelles.

5.4 Coordination du Service des technologies de l'information

La coordination du Service des technologies de l'information (STI) porte les responsabilités de RSI et de COGI. Relevant de la direction générale, elle met en place le cadre de gestion de l'utilisation des TI et de la sécurité de l'information et s'assure de son évolution en réponse aux besoins du Cégep et aux exigences gouvernementales.

La personne :

a) coordonne et évalue l'ensemble des activités touchant les TI au Cégep, en assure une vigie et en propose les orientations;

b) rapporte régulièrement les avancements, les orientations et les incidents au conseil de régie du Cégep et aux instances gouvernementales;

c) collabore à l'élaboration du contenu et au déploiement du plan de communication et du programme de sensibilisation et de formation en matière de sécurité de l'information;

d) procède aux enquêtes dans des cas de manquements graves ayant trait à la Politique;

e) tient à jour un registre des dérogations et des manquements à la présente Politique.

5.5 Service des technologies de l'information

Ce service gère et exploite quotidiennement les TI en plus d'intervenir dans la réalisation de projets de développement ou d'acquisition de systèmes d'information.

De plus, le Service des technologies de l'information :

a) 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;

b) applique des mesures préventives et de réaction appropriées à toute menace ou à tout incident de sécurité de l'information;

c) participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente Politique et autorisées par la direction générale;

d) collabore à la production d'outils de communication visant à sensibiliser et à former les utilisatrices et les utilisateurs.

5.6 Conseillère ou conseiller pédagogique en technologie de l'information

En collaboration avec le STI, cette personne conseille, accompagne et oriente le personnel enseignant dans une utilisation efficace et sécuritaire des TI dans l'enseignement et pour l'apprentissage et l'informe, le cas échéant, des éléments contenus dans la présente Politique.

5.7 Service de l'entretien des bâtisses et des terrains

Ce service participe au processus d'identification et à la mise en place des mesures de sécurité physique nécessaires afin de protéger adéquatement les actifs informationnels du Cégep.

5.8 Direction des ressources humaines

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

Elle transmet périodiquement au STI 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.

La DRH est aussi responsable de faire connaître à chaque nouvelle personne embauchée la Politique relative à l'utilisation des technologies de l'information et des communications et des 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.

5.9 Responsable de logiciel institutionnel

La personne responsable de logiciel institutionnel veille à l'accessibilité, à l'utilisation adéquate et à la sécurité du logiciel institutionnel sous sa responsabilité. Cette personne participe et collabore activement à l'analyse du risque et à la mise en œuvre de toute mesure visant à améliorer l'utilisation et la sécurité du logiciel dont il ou elle a la responsabilité. Elle gère le cycle de vie du logiciel en plus de s'assurer du respect de l'attribution des droits d'accès.

5.10 Utilisatrices et utilisateurs

Le respect de la présente Politique incombe à tous les utilisatrices et les utilisateurs des actifs informationnels du Cégep. Chacune et chacun doit s'y conformer ainsi qu'à tout autre document faisant partie du cadre de gestion.

À cette fin, l'utilisatrice ou l'utilisateur doit :

a) utiliser seulement les droits d'accès qui lui sont attribués et autorisés;

b) utiliser les actifs informationnels qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et dans le but auquel ces actifs sont destinés;

c) conserver confidentiellement ses codes d'accès et ses mots de passe, puisqu'il ou elle est responsable en tout temps des actions effectuées grâce à ceux-ci;

d) respecter les mesures en place ainsi que la néthique et la nétiquette;

e) préserver les actifs informationnels et ne pas modifier leur configuration;

f) signaler au personnel enseignant ou cadre responsable de son unité tout incident susceptible de constituer un manquement à la présente Politique;

g) utiliser les actifs informationnels de façon à assurer leur sécurité, leur pérennité et leur durabilité;

h) prendre connaissance des informations transmises par le Cégep concernant la sécurité et l'utilisation des technologies de l'information.

Article 6 – Sanctions

Dans le cas d'une utilisation inappropriée des TI, le Cégep pourra demander au contrevenant ou à la contrevenante de retirer le contenu jugé non sécuritaire, discriminatoire, diffamatoire ou non conforme à la présente Politique.

Selon la gravité des actes commis, il pourra également imposer une sanction pouvant aller jusqu'au renvoi du Cégep, pour l'étudiant ou l'étudiante, et une mesure disciplinaire pouvant aller jusqu'au congédiement pour le membre du personnel, et ce, conformément au Règlement n° 3 relatif à certaines conditions de vie au Cégep de Sherbrooke et aux mécanismes prévus aux conventions collectives. Enfin, l'établissement pourra rapporter la situation aux services de police si la situation le justifie.

Article 7 – Révision

La présente Politique et le cadre de gestion doivent être révisés, minimalement tous les cinq ans, et ce, afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques, environnementaux et des risques associés à l'évolution des menaces.

Article 8 – Entrée en vigueur

La présente Politique entre en vigueur le 21 mars 2019.