Cadre de gestion de la sécurité de l'information

Adopté par la Direction Générale le 28 août 2018

CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

TABLE DES MATIÈRES

Article 1 PRÉAMBULE

Le *Cadre de gestion de la sécurité de l'information* vient en complément de la *Politique sur la sécurité de l'information (POL-15).* Il vise à renforcer la gouvernance de la sécurité de l'information du Cégep, en décrivant les rôles et responsabilités nécessaires à une gestion intégrée de la sécurité de l'information. Le présent document a été conçu à partir du *Guide d'élaboration d'un cadre de gestion de la sécurité de l'information* rédigé par le gouvernement du Québec.

L'entrée en vigueur de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale* crée des obligations aux établissements en leur qualité d'organismes publics. Ainsi, la *Directive sur la sécurité de l'information gouvernementale* oblige les organismes publics à adopter et à mettre en œuvre un cadre de gestion de la sécurité de l'information, de le maintenir à jour et d'en assurer l'application.

Article 2 DÉFINITIONS

a) « Actif informationnel »
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 des technologies de l'information (logiciels, progiciels, didacticiels, banques 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.

b) « Utilisateur »
Tout le personnel, toute personne physique ou morale qui, à titre d'employé, d'étudiant, de consultant, de partenaire, de fournisseur ou d'invité, utilise les actifs informationnels du Cégep.

c) « Responsable d'actifs informationnels »
Le membre du personnel cadre 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.

Article 3 CADRE LÉGAL ET ADMINISTRATIF

Le *Cadre de gestion de la sécurité de l'information* s'inscrit dans un contexte légal principalement constitué de :

- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) et ses règlements;
- la *Directive sur la sécurité de l'information gouvernementale*;
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- la *Loi concernant le cadre juridique des technologies de 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) et ses règlements;
- la *Loi sur les archives* (RLRQ, c. A-21.1);
- la *Loi sur le droit d'auteur* (RLRC, 1985, c. C-42).

Dans le cadre administratif du Cégep :

- la *Politique sur la sécurité de l'information (POL-15);*
- le *Règlement sur la protection des renseignements personnels* (R-07);
- le *Règlement concernant la gestion des documents administratifs et des archives* (R-11);

Article 4 CHAMP D'APPLICATION

Le présent Cadre de gestion s'applique à tous les utilisateurs de l'information du Cégep.

Article 5 RÔLES ET RESPONSABILITÉS

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

5.1 PRINCIPAUX INTERVENANTS

5.1.1 Conseil d'administration

Le Conseil d'administration adopte la *Politique sur la sécurité de l'information* ainsi que toute modification à celle-ci. Le Conseil d'administration nomme le Responsable de la sécurité de l'information (RSI) tel que requis par la loi. Il est informé des actions du Cégep en matière de sécurité de l'information.

5.1.2 Directeur général

Le directeur général doit s'assurer du respect des lois et des règles de sécurité de l'information et est responsable de l'application de la *Politique sur la sécurité de l'information* et *du Cadre de gestion de la sécurité de l'information*.

- Il autorise, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la Politique ou du Cadre de gestion, d'une directive ou d'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;
- Il autorise une enquête lorsqu'il y a ou pourrait y avoir transgression de la Politique.

5.1.3 Direction générale

La direction générale du Cégep adopte des mesures visant à favoriser l'application de la Politique sur la sécurité de l'information et des obligations légales du Cégep en matière de sécurité de l'information. Ainsi, elle détermine les orientations stratégiques, les plans d'action et reçoit les bilans de sécurité de l'information. Elle désigne les responsables des actifs informationnels.

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

Le responsable de la sécurité de l'information (RSI) est nommé par le Conseil d'administration. Il relève du directeur général au sens du *Cadre gouvernemental de gestion de la sécurité de l'information.* Cette personne :

- élabore et propose le *Cadre de gestion de la sécurité de l'information* du Cégep et rend compte de son implantation à la Direction générale;
- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les règles et les bonnes pratiques en matière de sécurité de l'information et propose des mises à jour de 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 à 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 relatives à des transgressions réelles ou présumées ayant trait à la Politique, à la suite de l'autorisation du directeur général;
- tient à jour le registre des dérogations et le registre des cas de contravention à la présente Politique;
- 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.

5.1.5 Direction des technologies informatiques

En matière de sécurité de l'information, la Direction des technologies informatiques s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels elle intervient, elle :

- 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 systèmes d'information faisant appel aux technologies de l'information;
- applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information;
- participe à l'exécution des enquêtes informatiques relatives à des contraventions réelles ou apparentes à la *Politique sur la sécurité de l'information*, autorisées par le directeur général.

5.1.6 Direction des finances et des ressources matérielles

La Direction des finances et des ressources matérielles, avec le responsable de la sécurité de l'information, voit à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

5.1.7 Direction des ressources humaines et des affaires corporatives

En matière de sécurité de l'information, la Direction des ressources humaines et des affaires corporatives obtient de tout nouvel employé du Cégep, après lui en avoir montré la nécessité, son engagement au respect de la *Politique sur la sécurité de l'information.*

5.1.8 Responsable d'actifs informationnels

Le responsable d'actifs informationnels est le gestionnaire 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 une partie de sa responsabilité à un autre gestionnaire du service.

Le responsable d'actifs informationnels :

- informe le personnel relevant de son autorité et les tiers avec lesquels transige le service sous sa responsabilité, de la *Politique sur la sécurité de l'information* et des dispositions du *Cadre de gestion de la sécurité de l'information* 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 autorisé en conformité avec la *Politique sur la 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 sur la sécurité de l'information* et tout autre élément du *Cadre de gestion*;
- rapporte à la Direction des technologies informatiques 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 responsable de la sécurité de l'information (RSI) tout problème lié à l'application de la *Politique sur la sécurité de l'information*, dont toute contravention réelle ou apparente d'un utilisateur en ce qui a trait à l'application de cette Politique.

5.1.9 Utilisateurs

La responsabilité de la sécurité de l'information du Cégep 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 *Politique sur la sécurité de l'information* 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, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- respecter les mesures de sécurité mises en place, sans les contourner, sans modifier leur configuration ou les désactiver;
- signaler au responsable du service ou du département, tout incident susceptible de constituer une contravention à la *Politique sur la sécurité de l'information* ou de constituer une menace à la sécurité de l'information du Cégep;
- collaborer à toute intervention visant à indiquer ou à atténuer une menace à la sécurité de l'information ou à un incident de sécurité de l'information.

Aussi, tout utilisateur du Cégep doit se conformer aux politiques et aux directives en vigueur au Cégep dans le cadre de ses activités professionnelles ou d'études lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

5.2 AUTRES INTERVENANTS

5.2.1 Coordonnateur sectoriel de la gestion des incidents (CSGI)

Outre sa participation active au réseau d'alerte gouvernemental, le CSGI :

- contribue à la mise en place du processus de gestion des incidents de sécurité de l'information;
- assure l'échange d'information entre le Cégep et le CERT/AQ et met en œuvre les stratégies de réaction appropriées;
- contribue aux analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité et met en œuvre les solutions appropriées;
- collabore étroitement avec le responsable de la sécurité de l'information (RSI) et lui fournit le soutien technique nécessaire à l'exercice de ses responsabilités.

5.2.2 Responsable de la gestion documentaire

Le responsable de la gestion documentaire :

- s'assure qu'à toutes les étapes du cycle de vie de l'information, les systèmes d'information ont les qualités nécessaires pour permettre une saine gestion des données et le respect des lois;
- collabore étroitement avec les responsables d'actifs informationnels ainsi qu'avec le Coordonnateur sectoriel de gestion des incidents (CSGI) en vue de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

5.2.3 Responsable de l'accès à l'information et de la protection des renseignements personnels

Le responsable de l'accès à l'information et 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). À ce titre, il :

- communique au Responsable de la sécurité de l'information (RSI) les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles;
- contribue à assurer la cohérence et l'harmonisation des interventions avec la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels.

Article 6 DIFFUSION ET MISE À JOUR DU CADRE DE GESTION

Le responsable de la sécurité de l'information (RSI), en collaboration avec la Direction du développement institutionnel et des communications, est responsable de la diffusion et de la mise à jour du cadre de gestion.

Le *Cadre de gestion de la sécurité de l'information* est révisé et modifié au besoin.

Article 7 ENTRÉE EN VIGUEUR

Le présent Cadre de gestion entre en vigueur dès son adoption par la Direction générale.