N° BOG-DG-01

Titre :	**POLITIQUE-CADRE SUR LA SÉCURITÉ DE L'INFORMATION**
CLASSIFICATION :	Direction générale
ADOPTION INITIALE :	11 avril 2018 (BOG 492.6.6)

Cette politique a été adoptée en anglais. En cas de divergence la version anglaise prévaut sur la version française

Objectifs

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* et la *Directive sur la sécurité de l'information gouvernementale* exigent l'adoption d'une politique-cadre en matière de sécurité de l'information.

Cette politique-cadre permet de mettre en place des mesures adéquates pour garantir :

- la *confidentialité* de l'information, en limitant sa divulgation et son utilisation aux seules personnes autorisées;
- l'*intégrité* de l'information, en assurant sa pérennité et en empêchant sa destruction ou son altération injustifiée;
- la *disponibilité* de l'information, en y garantissant l'accès en temps opportun et aux seules personnes autorisées.

Article 1 Contexte juridique

La présente politique-cadre doit être appliquée conformément aux lois, règlements, réglementations et politiques applicables, y compris, mais sans s'y limiter :

- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, G-1.03) et la *Directive sur la sécurité de l'information gouvernementale*;
- le *Cadre gouvernemental de gestion de la sécurité de l'information*;
- la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, 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, A-21.1);
- la *Charte des droits et libertés de la personne* (RLRQ, C-12);
- le *Code civil du Québec* (RLRQ, CCQ-1991);
- le *Code criminel* (LRC, C-46);
- les politiques de sécurité informatique (*IT Security Policy*, IST-01) et de gestion des incidents informatiques (*IT Incident Management Policy*, IST-05) du Collège.

Article 2 Champ d'application

Toute information que le Collège recueille, produit ou conserve dans le cadre de ses activités est soumise à la présente politique-cadre. L'information peut être conservée sous forme électronique ou sur papier, et peut se trouver physiquement à l'intérieur ou à l'extérieur des locaux du Collège.

Cette politique s'applique au personnel, à la population étudiante et aux tiers qui utilisent cette information.

Article 3 Cadre de gestion de la sécurité

La gestion de la sécurité de l'information repose sur trois composantes : la gestion de l'accès, la gestion des risques et la gestion des incidents.

3.1. Gestion de l'accès

Des mesures sont en place pour garantir que l'accès à l'information, sa divulgation et son utilisation sont strictement réservés aux personnes autorisées. Ces mesures protègent l'intégrité et la confidentialité de l'information, en accordant une attention particulière aux renseignements personnels.

L'efficacité de la gestion de l'accès repose sur l'attribution de responsabilités et la reddition de comptes à tous les niveaux du Collège.

3.2. Gestion des risques

La gestion des risques liés à la sécurité de l'information fait partie du processus global de gestion des risques du Collège.

L'analyse des risques guide l'acquisition, le développement et l'exploitation des systèmes d'information, en précisant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du Collège.

3.3. Gestion des incidents

Le Collège déploie des mesures pour assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires pour atteindre les objectifs suivants :

- limiter les incidents liés à la sécurité de l'information;
- gérer ces incidents de manière adéquate afin d'en minimiser les conséquences et de rétablir les opérations.

Les incidents de portée gouvernementale sont définis dans la *Directive sur la sécurité de l'information gouvernementale comme des événements qui compromettent la disponibilité, l'intégrité ou la confidentialité de l'information gouvernementale et qui nécessitent une intervention concertée.* Ils sont rapportés comme le prévoit la directive.

Dans le cadre de la gestion des incidents, le Collège peut exercer ses pouvoirs et prérogatives à l'égard de toute utilisation abusive de l'information qu'il détient ou de ses systèmes d'information.

Article 4 Rôles et responsabilités

4.1. Conseil d'administration

Le conseil d'administration adopte la présente politique-cadre et ses modifications et délègue son application à la direction générale. Il nomme également le ou la responsable de la sécurité de l'information, comme le prévoit le Cadre gouvernemental de gestion de la sécurité.

4.2. Direction générale

La direction générale est responsable de l'application de la présente politique. En particulier, la direction générale :

- recommande la présente politique et les modifications à y apporter au conseil d'administration;
- encadre le ou la responsable de la sécurité de l'information dans l'exécution de son mandat;
- informe le conseil d'administration des actions liées à la sécurité de l'information, telles que l'évaluation des risques, les plans d'action, etc;
- autorise exceptionnellement les dérogations à la présente politique;
- applique des sanctions en cas de violation de la présente politique.

4.3. Responsable de la sécurité de l'information

Outre son mandat défini dans le *Cadre gouvernemental de la gestion de la sécurité de l'information*, le ou la responsable de la sécurité de l'information assure la liaison avec le ministère et assiste la direction générale dans la mise en œuvre de la présente politique. En particulier, le ou la responsable de la sécurité de l'information :

- recommande à la direction générale la présente politique et les modifications à y apporter, ainsi que d'autres directives, plans d'action, etc., le cas échéant;
- mène des enquêtes sur les cas éventuels de violation de la présente politique;
- signale les infractions à la politique à la direction générale;
- coordonne et assure la cohérence des actions menées par les différents propriétaires d'information, tout en tenant compte des aspects de la gestion des contrats, de l'accès et de la protection des renseignements personnels, et de la gestion des documents;
- veille à ce que le Collège participe au processus gouvernemental de gestion des risques et de déclaration des incidents;
- établit le cadre de gestion de la sécurité;
- met en place un programme de formation et de sensibilisation à la sécurité de l'information.

4.4. Direction des études et autres directions

La direction des études et les autres directions sont chargées de veiller à ce que les activités de leurs unités soient conformes à la politique, et à ce qu'un effort proportionnel au risque soit déployé pour protéger l'information. Elles collaborent activement avec le ou la responsable de la sécurité de l'information pour évaluer les risques, mettre en œuvre de nouvelles mesures et signaler toute menace potentielle portée à leur connaissance.

Les directions suivantes ont des responsabilités supplémentaires :

- la direction des technologies et systèmes d'information veille à ce que les exigences de sécurité soient respectées dans les systèmes d'information existants ainsi que lors de l'acquisition ou du développement de nouveaux systèmes;
- la direction des technologies et systèmes d'information applique les mesures appropriées de réponse aux menaces ou aux incidents en matière de sécurité de l'information, telles que l'interruption ou la révocation temporaire, lorsque les circonstances l'exigent;
- la direction des ressources matérielles participe à l'identification des mesures de sécurité physique visant à protéger de manière adéquate les actifs informationnels du Collège;
- la direction des ressources humaines obtient un engagement des nouvelles et nouveaux employés du Collège à respecter la présente politique.

4.5. Utilisateurs et utilisatrices

Lorsqu'ils accèdent à de l'information ou lorsqu'ils la traitent, les utilisateurs et utilisatrices doivent procéder de manière à la protéger. Ils doivent utiliser leur accès uniquement aux fins auxquelles cet accès est destiné. Ils doivent signaler les incidents qui pourraient constituer une menace pour la sécurité de l'information et collaborer aux enquêtes.

4.6. Comité de sécurité de l'information

L'objectif de ce comité de travail est d'aider le ou la responsable de la sécurité de l'information à mettre en œuvre la présente politique, le cadre de gestion de la sécurité, les plans d'action ainsi que les programmes de formation et de sensibilisation.

Article 5 Sanctions

Toute personne salariée ou étudiante qui contrevient à la présente politique ou aux mesures de sécurité de l'information qui s'y rattachent est passible de sanctions selon la nature, la gravité et les conséquences de l'infraction en vertu du règlement ou des règles disciplinaires applicables (y compris celles des conventions collectives et les règles du Collège). La personne salariée ou étudiante peut être tenue personnellement responsable, même en cas de négligence ou d'omission, si l'infraction entraîne une protection insuffisante de l'information.

De même, toute violation de la présente politique perpétrée par un organisme tiers ou un individu qui n'est pas employé ou étudiant, est passible des sanctions prévues dans le contrat qui le lie au Collège ou en vertu des dispositions de la législation applicable.

Article 6 Dispositions finales

Cette politique entre en vigueur à la date d'adoption.