COLLÈGE DE
BOIS-DE-BOULOGNE

# POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

*Adoptée au conseil d'administration*
*lors de la 350e assemblée, le 2 décembre 2020*
*(résolution no 3319)*

# TABLE DES MATIÈRES

## PRÉAMBULE

Cette politique constitue un élément essentiel à la gouvernance de l'information permettant ainsi au Collège de Bois-de-Boulogne d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qui est traitée, produite et communiquée. Cette information est très vaste et peut exister sur support papier ou technologique. Elle comprend, entre autres, les renseignements personnels des étudiants et des membres du personnel, la propriété intellectuelle produite par les enseignants et les chercheurs, ainsi que la documentation interne stratégique et administrative.

Comme toute autre institution d'enseignement supérieur, le Collège fait face à une multitude de menaces pouvant porter atteinte à la confidentialité, l'intégrité et la disponibilité de son information. Ces menaces, dont la nature est en constante évolution, comprennent, entre autres, le vol d'identité et d'information confidentielle, la fraude, l'espionnage industriel et le vol de propriété intellectuelle, l'utilisation, la divulgation et la destruction d'information, les défaillances techniques, les événements naturels et l'erreur humaine.

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03) et la *Directive sur la sécurité de l'information gouvernementale* font état des obligations en cette matière auxquelles doivent se conformer tous les établissements collégiaux en leur qualité d'organismes publics.

## 1. DÉFINITIONS

**1.1 Actif informationnel** – *La Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., chapitre C-1.1) définit l'actif informationnel sans égard au support comme étant : « Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles. » Cette même loi assimile au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

**1.2 Confidentialité** – Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

**1.3 Cycle de vie de l'information** – L'ensemble des étapes que franchit une information et qui vont de sa création en passant par son enregistrement, son transfert, sa

consultation, son traitement et sa transmission, jusqu'à sa conservation ou à sa destruction, en conformité avec le calendrier de conservation[1].

**1.4 Disponibilité** – Propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

**1.5 Intégrité** – Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

## 2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Collège 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 Collège 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;
- 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 utilisé offre 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 et aux fins prévues, surtout si elle constitue des renseignements personnels.

La politique soutient la mise en œuvre du cadre de gestion en matière de sécurité de l'information et renforce le maintien de systèmes de contrôles internes offrant une assurance raisonnable de conformité à l'égard des lois, directives et pratiques gouvernementales en la matière.

## 3. CADRE LÉGAL ET ADMINISTRATIF

La *Politique sur la sécurité de l'information* s'inscrit principalement dans un contexte régi par les encadrants suivants :

- *Charte des droits et libertés de la personne* (LRQ, chapitre C-12);
- *Code civil du Québec* (LQ, 1991, chapitre 64);
- *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03);

[1] Pour les références au plan de classification et au calendrier de conservation, voir la Politique de gestion des archives.

- *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014);
- *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1);
- *Loi sur les archives* (LRQ, chapitre A-21.1);
- *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42;
- *Code criminel* (LRC, 1985, chapitre C-46);
- *Politique de gestion des archives* du Collège de Bois-de-Boulogne;
- *Politique relative à l'utilisation des technologies de l'information et des communications* du Collège de Bois-de-Boulogne.

## 4. CHAMP D'APPLICATION

La présente politique s'applique aux utilisateurs de l'information, c'est-à-dire à tous les membres du personnel, peu importe leur statut, et à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur ou d'étudiant, utilise les actifs informationnels du Collège.

Les actifs informationnels visés sont ceux que le Collège détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

Les activités visées par la *Politique sur la sécurité de l'information* sont la collecte, la consultation, la production, la transmission, la conservation et la destruction de l'information et des actifs informationnels, peu importe leur support, leur emplacement et le moyen de communication.

## 5. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du Collège en matière de sécurité de l'information sont les suivants :

**5.1 Protection de l'information** – Le Collège 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 Collège 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 confidentialité et 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.

**5.2 Imputabilité** – Chaque direction ou service administratif est imputable de la gestion des risques à la sécurité de l'information en sa qualité de propriétaire de l'information. Cette imputabilité s'applique aux actifs informationnels, aux processus et aux systèmes sous sa responsabilité ou son contrôle, incluant ceux délégués à un tiers.

**5.3 Proportionnalité** – Des mesures raisonnables sont mises en place pour garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels, à un coût proportionnel à la sensibilité de l'information et aux risques sous-jacents, différents types d'information pouvant nécessiter des niveaux de protection différents. D'autre part, les mesures mises en place pour protéger les actifs informationnels ne doivent pas nuire à la mission du Collège.

**5.4 Sensibilisation et formation** – Le Collège 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.

**5.5 Droit de regard** – Le Collège 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.

## 6. CADRE DE GESTION

La politique confère la reconnaissance et la légitimité à la direction du Collège de définir des directives, des procédures, des guides en lien avec la sécurité de l'information. L'ensemble de ces documents fait partie du cadre de gestion qui a pour objectif d'aligner les opérations dans l'esprit de la présente politique. Puisque le domaine de la sécurité informationnelle est en constante évolution, le cadre de gestion permettra au Collège de s'adapter aux nouvelles réalités de façon efficace et continue de façon à poursuivre sa mission tout en répondant à ses obligations.

## 7. RÔLES ET RESPONSABILITÉS

La présente politique détermine les obligations en matière de sécurité de l'information attribuées, notamment, au responsable organisationnel de la sécurité de l'information, aux gestionnaires d'entités administratives et aux utilisateurs.

**7.1 Conseil d'administration** – Le conseil d'administration (ci-après le CA) adopte la *Politique sur la sécurité de l'information* ainsi que toute modification à celle-ci. Le conseil est régulièrement informé des actions du Collège en matière de sécurité de

l'information.

**7.2 Comité en sécurité de l'information** – Le rôle du comité en sécurité de l'information est d'être la principale instance en matière de sécurité de l'information afin d'assurer la coordination, la concertation et la cohérence des actions en cette matière. Il soutient le responsable de la sécurité de l'information (ci-après le RSI) en regard des obligations de gouvernance et de gestion de la sécurité de l'information définies dans la *Directive sur la sécurité de l'information gouvernementale.*

Ce comité est chargé en particulier :

- De recommander, pour approbation, les documents stratégiques, destinés aux autorités ou affectant de façon importante l'ensemble du personnel de l'organisation;
- D'approuver les documents de nature tactique, diffusés à l'interne et ayant peu d'impact sur le personnel;
- De prendre connaissance des informations administratives ou techniques;
- D'émettre des recommandations pour la mise en place de mesures de sécurité.

**7.3 Directeur général** – Le directeur général veille à l'application de la *Politique sur la sécurité de l'information*.

Plus précisément, il a pour tâches :

- D'encadrer le RSI dans la réalisation de son mandat;
- De déléguer, au besoin, certaines responsabilités au secrétaire général pour la gestion de l'information;
- De faire adopter par le CA 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, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information lorsque la mission du Collège est compromise.
- D'autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la politique;
- De tenir à jour le registre des dérogations et le registre des cas de contravention à la présente politique.
- De mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels à sa clientèle, selon un temps prévu.

**7.4 Responsable de la sécurité de l'information** – La fonction du Responsable de la sécurité de l'information est déléguée à un cadre par le conseil d'administration. Le RSI relève du directeur général au sens du cadre gouvernemental de gestion de la sécurité de l'information. Cette personne met en place le cadre de gestion de la sécurité de l'information et s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins. Il est nommé par le conseil d'administration.

Le RSI a plus précisément pour tâches :

- D'élaborer et de proposer le programme de sécurité de l'information du Collège, de rendre compte de son implantation au comité de direction;
- De formuler 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 et de mettre à jour la politique;
- D'assurer la coordination et la cohérence des actions menées au sein du Collège en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans les unités;
- De produire les plans d'action, les bilans et les redditions de comptes du Collège en matière de sécurité de l'information;
- De proposer des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;
- De s'assurer de la déclaration par le Collège des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- De collaborer à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et de veiller au déploiement de ceux-ci;
- D'assurer la responsabilité des enquêtes dans des transgressions sérieuses ayant trait vraisemblablement à la politique à la suite de l'autorisation du dirigeant de l'organisme;
- D'assurer 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.

**7.5 Direction des ressources informationnelles et des technologies numériques** – En matière de sécurité de l'information, la Direction des ressources informationnelles et des technologies numériques (ci-après la DRITN) 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;
- Elle applique des mesures appropriées à toute menace ou à tout incident de sécurité de l'information;
- Elle participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par le directeur général.

**7.6 Responsables d'actifs informationnels** – Les responsables d'actifs informationnels sont les cadres détenant l'autorité au sein de leur direction ou service et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous leur responsabilité. Les responsables d'actifs informationnels peuvent déléguer la totalité ou bien une partie de leur responsabilité à un autre membre de leur direction ou service.

Les responsables d'actifs informationnels :

- Informent le personnel relevant de leur autorité et les tiers avec lesquels transige le service de la *Politique sur la sécurité de l'information* et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer;
- S'assurent que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;
- Collaborent activement à la catégorisation de l'information de la direction ou service sous sa responsabilité et à l'analyse de risques;
- Voient 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 sur la sécurité de l'information* et de tout autre élément du cadre de gestion;
- S'assurent 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 voient 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;
- Rapportent à la DRITN toute menace ou tout incident afférant à la sécurité de l'information;
- Collaborent 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;
- Rapportent au directeur général 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.

**7.7 Utilisateurs** – La responsabilité de la sécurité de l'information du Collège incombe à tous les utilisateurs des actifs informationnels du Collège.

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 Collège 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;
- Participer à la catégorisation de l'information de son service;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- Signaler au responsable des actifs informationnels de son unité tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du Collège;
- Collaborer à toute intervention visant à indiquer ou à mitiger une menace à la sécurité de l'information ou un incident de sécurité de l'information;

Aussi, tout utilisateur du Collège doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation 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.

## 8. SANCTIONS

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l'information qui en découlent, 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 notamment celles des conventions collectives de travail et du *Règlement no 5 sur les comportements*.

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 Collège ou en vertu des dispositions de la législation applicable en la matière.

## 9. DIFFUSION

Le RSI, assisté du comité de travail pour la sécurité de l'information, est responsable de la diffusion de la présente politique auprès de toutes les personnes et organismes concernés.

Toute modification ou abrogation de la présente politique doit être adoptée par le conseil d'administration du Collège et respecter les dispositions des lois et des règlements y afférant. La révision de la politique s'effectue lors de changements significatifs pouvant en affecter les dispositions ou au plus tard cinq ans après son adoption.

## 10. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration.