Collège Lionel-Groulx

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Adoption par le conseil d'administration le 28 novembre 2017

TABLE DES MATIÈRES

1. DÉFINITIONS

Actifs informationnels :	Tous éléments contenant de l'information ayant une valeur pour le gouvernement ou pour l'organisation. Fait aussi référence à des biens physiques tels que les appareils, systèmes, téléphones, support de toutes natures, bases de données, logiciels, etc.
CERT/AQ :	Désigne l'équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise à portée gouvernementale (*Computer Emergency Response Team/Area Quebec*).
COGI-réseau :	Désigne le Coordonnateur Organisationnel de Gestion des Incidents.
Collège :	Désigne la personne morale Collège Lionel-Groulx.
CSGI :	Désigne le Coordonnateur Sectoriel de la Gestion des Incidents.
DG :	Désigne la Direction générale.
DIIM :	Désigne la Direction des Infrastructures informationnelles et matérielles.
DRH :	Désigne la Direction des Relations Humaines
RSI :	Désigne le Responsable de la Sécurité de l'Information
Utilisateur :	Désigne toute personne physique ou morale qui utilise les actifs informationnels.

2. PRÉAMBULE

La présente Politique constitue le cadre de référence en ce qui a trait à la protection de l'information créée ou reçue par le Collège Lionel-Groulx. La nature de ces informations est diverse. Il s'agit, entre autres, de renseignements confidentiels concernant les étudiants ou le personnel de l'institution, d'information professionnelle assujettie à des droits de propriétés intellectuelles, d'informations stratégiques ou opérationnelles de l'administration du Collège, etc.

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.

3. OBJECTIFS

La présente Politique a pour objectif de définir les balises permettant au Collège Lionel-Groulx de 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.
- 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 utilisé offre la stabilité et la pérennité voulues.
- Assurer la confidentialité de l'information en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées.

Par conséquent, le Collège met en place cette Politique dans le but d'orienter et de déterminer sa vision qui sera détaillée dans le cadre de gestion de la sécurité de l'information de l'institution.

Le cadre de gestion de la sécurité de l'information renforce les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et des directives gouvernementales, ainsi qu'aux autres besoins du Collège en matière du risque associé à la protection de l'information.

4. CADRE LÉGAL ET ADMINISTRATIF

La présente Politique s'inscrit principalement dans un contexte régi par :

- La *Charte des droits et libertés de la personne* (LRQ, chapitre C-12).
- Le *Code civil du Québec* (LRQ, 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* (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).
- Le *Code criminel* (LRC, 1985, chapitre C-46).

- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1, r.2).
- La *Directive sur la sécurité de l'information gouvernementale* (LRC, 1985, chapitre C-42).
- La *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42).

5. CHAMP D'APPLICATION DE LA POLITIQUE

La Politique s'applique sans exception à tous les utilisateurs des ressources et des actifs informationnels du Collège. Elle énonce les principes venant encadrer l'octroi des accès requis pour la réalisation des différentes activités du Collège.

L'information dont il est question dans la présente Politique fait référence aux renseignements que le Collège détient dans le cadre de ses opérations, que la conservation de ceux-ci soit assurée par l'institution ou par un tiers.

Tous les supports, incluant le papier, sont visés par cette Politique.

6. PRINCIPES DIRECTEURS

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

a) S'assurer de bien connaître l'information à protéger, en identifier les responsables ainsi que la caractéristique de sécurité.
b) Se conformer aux normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et recourir à des barèmes de comparaison avec des organismes ou des institutions similaires.
c) Adhérer à une approche basée sur le risque acceptable.
d) Protéger rigoureusement les renseignements personnels ainsi que les informations confidentielles.
e) Reconnaître l'importance d'évaluer régulièrement les risques, de mettre en place des mesures proactives de sécurité et des méthodes de détection des usages abusifs ou inappropriés de l'information ainsi que de définir des actions d'éradication des menaces ou de recouvrement des activités compromises.
f) Protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction.
g) Adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de sécurité de l'information avec le réseau de l'éducation et les organismes publics.

h) Adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.
i) S'assurer que chaque employé ait accès au minimum d'information requise pour accomplir l'ensemble des tâches inhérentes à sa fonction.
j) Communiquer de façon transparente au sujet des menaces pouvant affecter les actifs informationnels afin que tous soient en mesure de comprendre la nécessité d'appliquer les normes de sécurité de la manière prescrite, qu'ils soient en mesure de reconnaître les incidents de sécurité.
k) Mettre en place un plan de continuité des opérations en vue de rétablir les services essentiels aux utilisateurs selon le délai prévu.

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 Collège 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* s'articule autour de trois axes fondamentaux de gestion, soit :

- La gestion des accès.
- La gestion des risques.
- La gestion des incidents.

7.1 Gestion des accès

La gestion des accès se doit clairement balisée. Des mesures sont mises en place afin de protéger l'intégrité et la confidentialité des informations détenues par l'institution. L'efficacité des mesures de sécurité de l'information repose sur le contrôle de l'attribution des droits d'accès ainsi que sur l'imputabilité des utilisateurs à tous les niveaux de personnel du Collège.

7.2 Gestion des risques

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître avec justesse 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 Collège. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques. 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 :

a) De la nature de l'information et son importance.
b) Des probabilités d'incidents, d'erreurs ou de malveillance.
c) Les conséquences liées aux risques.
d) Du niveau de risque acceptable pour le Collège.

7.3 Gestion des incidents

Le Collège déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. Ces mesures visent à :

- Limiter l'occurrence des incidents en matière de sécurité de l'information.
- Gérer adéquatement les incidents afin de minimiser les conséquences et rétablir rapidement les services.

Les incidents de sécurité de l'information à portée gouvernementale doivent être déclarés par le CERT/AQ conformément à la *Directive sur la sécurité de l'information gouvernementale*.

En ce qui a trait à la gestion des incidents, le Collège peut exercer ses pouvoirs et ses prérogatives quant à l'utilisation inappropriée de l'information ou des systèmes d'information qu'il détient.

8. RÔLES ET RESPONSABILITÉS

La présente Politique confie la gestion de la sécurité de l'information du Collège à des instances, à des comités et à des personnes selon les fonctions particulières qu'ils occupent dans l'organisation.

8.1 Conseil d'administration

Le conseil d'administration adopte la Politique de sécurité de l'information ainsi que toutes modifications qui y sont apportées à celle-ci. Cette instance procède également à la nomination du Responsable de la Sécurité Informatique (RSI).

8.2 Comité de direction

Le comité de direction détermine les mesures favorisant l'application de la présente Politique. Il détermine les orientations stratégiques, les plans d'action et les bilans qui en découlent. Cette instance peut adopter des directives et des procédures qui viendront préciser ou soutenir l'application de la Politique.

8.3 Direction générale

La Direction générale veille à l'application de la présente Politique. Elle aura pour tâche :

a) D'encadrer le service de qui relève le RSI dans la réalisation de son mandat.
b) De déléguer certaines responsabilités au secrétaire général ou tout autre officier pour la gestion de l'information.
c) 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 compte en matière de sécurité de l'information.
d) D'autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente Politique ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement en lien avec la mission du Collège.
e) D'autoriser une enquête lorsqu'il y a transgression ou apparence de transgression à la présente Politique.
f) De tenir à jour le registre des dérogations ainsi que le registre des cas de contravention à la Politique.

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

La fonction de RSI est déléguée à un cadre par le conseil d'administration. Le RSI relève de la Direction générale ou d'un officier dûment mandaté à cette fin au sens du *Cadre gouvernemental de gestion de la sécurité de l'information*. Le RSI devra assurer la mise en place du cadre de gestion de la sécurité de l'information et s'assurer que le niveau de maturité de l'organisation en cette matière répond aux besoins.

Le RSI :

- Élabore et propose le programme de sécurité de l'information du Collège et rends compte de sa mise en œuvre au comité de direction.
- Formule des recommandations en ce qui concerne les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les bonnes pratiques et la mise à jour de la présente Politique.
- Assure la coordination et la cohérence des actions menées au Collège en matière de sécurité de l'information en conseillant les responsables des actifs informationnels.
- Produit les plans d'action, les bilans et effectue les redditions de compte en matière de sécurité de l'information.
- Propose des règles visant le respect des exigences en matière de sécurité de l'information à inclure dans les ententes de services et les contrats.
- S'assure de la déclaration par le Collège 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 à la mise en œuvre de ceux-ci.
- Procède aux enquêtes, après en avoir obtenu l'autorisation du dirigeant de l'organisme, lorsqu'il y a transgressions sérieuses des dispositions de la présente Politique.
- S'assure des veilles normatives, juridiques, gouvernementales et technologiques en matière de sécurité de l'information.

8.5 Coordonnateur sectoriel de la gestion des incidents (CSGI)

La fonction de RSI est déléguée par le comité de direction à un cadre ayant les compétences en cette matière. Le CSGI relève de la DIIM, agit au point de vue tactique et opérationnel et apporte son soutien au RSI notamment en ce qui a trait à la gestion des incidents et des risques. Il est répondant officiel du Collège auprès du CERT/AQ.

Le CSGI :

- Collabore étroitement avec le COGI du réseau de l'éducation.
- Collabore avec le RSI du Collège quant à l'élaboration de divers éléments stratégiques et tactiques en sécurité dont :
    - Un cadre de gestion.
    - Un registre d'autorité.
    - Une catégorisation des actifs.
    - Des mesures de sécurité pour les actifs critiques.
    - Un processus formel de gestion des risques en sécurité informatique.
    - Un processus formel de gestion des droits d'accès.
- Participe activement à la mise en place d'un réseau d'alertes.
- Participe, avec le COGI-réseau, au processus gouvernemental de gestion des incidents et au réseau d'alerte gouvernemental coordonné par le CERT/AQ.
- Élabore et met en œuvre, avec le soutien du COGI-réseau, un processus formel de gestion et de déclaration des incidents du Collège.
- Coordonne, avec le soutien du COGI-réseau, la gestion des incidents du Collège ainsi que celles à portée gouvernementale.
- Développe, met en place et évalue le plan de réponse aux incidents de sécurité du Collège.
- Mets en œuvre, en collaboration avec le COGI-réseau, les stratégies de réactions appropriées pour le Collège au moment d'un incident.
- Contribue aux analyses des risques, définit les menaces et les situations de vulnérabilité et met en œuvre des solutions appropriées pour le Collège.
- Contribue à l'évaluation de la sécurité des systèmes et des réseaux informatiques du Collège notamment par des exercices d'audit de sécurité et des tests d'intrusion aux systèmes jugés à risque.
- Élabore et procède à la mise à jour des guides traitant de la sécurité opérationnelle des systèmes et des réseaux de télécommunications mis en place au Collège.
- Assure une veille des risques, des menaces et des vulnérabilités.

Formule des recommandations en ce qui concerne les besoins, les priorités, les

8.6 Direction des infrastructures informationnelles et matérielles (DIIM)

En matière de sécurité de l'information, la DIIM s'assure du respect des obligations en matière de sécurité de l'information quant à l'acquisition, l'exploitation des systèmes d'information et la mise en œuvre de projet de développement.

- Elle participe activement à l'analyse des risques, à l'évaluation des besoins et à la détermination des mesures à mettre en œuvre en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information.

- Elle applique les mesures appropriées afin de protéger les actifs informationnels des menaces ou de limiter l'impact des incidents en matière de sécurité de l'information dont, entre autres, l'interruption ou la révocation temporaire de droits lorsque les circonstances l'exigent.
- Elle collabore aux enquêtes relatives à des contraventions réelles ou apparentes à la présente Politique.
- Elle identifie les mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Collège.

8.7 Direction des relations humaines (DRH)

En matière de sécurité de l'information, la DRH s'assure de diffuser la présente Politique à tout nouvel employé du Collège.

8.8 Responsable d'actifs informationnels (propriétaire)

Le responsable d'actifs informationnels est le cadre détenant l'autorité au sein d'un service et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous sa responsabilité. Il peut donc y avoir plusieurs responsables d'actifs informationnels dans un Collège. Le responsable d'actifs informationnels peut déléguer la totalité ou une partie de sa responsabilité à un autre membre du personnel de son service.

Le responsable d'actifs informationnels :

- Informe le personnel relevant de son 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.
- Collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse des risques.
- S'assure de 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 sous son autorité en conformité avec la *Politique sur la sécurité de l'information*.
- S'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tous processus d'acquisition et tout contrat de service sous sa responsabilité et voit à ce que les tiers s'engagent à respecter la présente Politique et tout élément du cadre de gestion.
- Rapporte à la Direction des infrastructures informationnelles et matérielles tout incident ou menace en matière de sécurité de l'information.

- Collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à corriger un incident de sécurité de l'information.
- Fait rapport à la Direction générale ou à tout autre officier dûment mandaté de tout problème lié à l'application de la présente Politique.

8.9 Utilisateurs

La responsabilité de la sécurité de l'information du Collège incombe à tous les utilisateurs des actifs informationnels. 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 la protéger.

À cette fin, l'utilisateur doit :

- Se conformer à la présente Politique sur la sécurité de l'information.
- 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.
- Signaler au responsable d'actifs informationnels de son service 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.

Les utilisateurs du Collège doivent se conformer aux politiques, règlements et directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles lorsqu'il est appelé à partager des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

9. SENSIBILISATION À L'INFORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté du Collège doivent être sensibilisés :

a) À la sécurité de l'information et des systèmes de l'information du Collège.
b) Aux conséquences d'une atteinte à la sécurité.
c) À leurs rôles et leurs responsabilités en cette matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. Il en sera de l'obligation des membres de la communauté collégiale d'y assister. De plus, des documents explicatifs seront mis à la disposition de tous sur le site Internet du Collège.

10. SANCTION

En cas de contravention à la Politique, l'utilisateur engage sa responsabilité personnelle. Il en est de même pour la personne qui, par négligence ou omission, fait en sorte que l'information n'est pas protégée adéquatement.

Toute contravention à la présente Politique peut mener à la suspension des privilèges d'accès aux ressources informationnelles du Collège. Des mesures administratives, disciplinaires ou légales pourront être entreprises auprès des contrevenants.

De même, toute contravention à la présente Politique perpétrée par un tiers est passible des sanctions prévues au contrat le liant au Collège ou en vertu des dispositions de la législation applicable en cette matière.

11. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

La Politique de sécurité de l'information sera révisée de façon périodique ou au besoin sur recommandation du comité de direction.

12. ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur le jour de son adoption par le conseil d'administration.