Collège d'Alma

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Adoptée au conseil d'administration le 16 juin 2025

TABLE DES MATIÈRES

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

PRÉAMBULE

Le Collège d'Alma reconnaît que l'information et les technologies qui la supportent sont essentielles à ses opérations courantes et à l'accomplissement de sa mission d'enseignement et de recherche, et vu la valeur administrative, légale et financière de ses actifs informationnels, ils doivent faire l'objet d'une évaluation continue, d'une utilisation et d'une protection appropriées et adéquates tout au long de leur cycle de vie, selon les bonnes pratiques en la matière de sécurité informationnelle et avec une approche de gestion des risques, quel qu'en soit le support ou l'emplacement.

L'application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre. G-1.03), de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, 2021, chapitre 25), et de la Directive gouvernementale sur la sécurité de l'information (2021) du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics, impose des obligations importantes aux établissements collégiaux.

Pour se conformer et répondre à ses obligations réglementaires et légales, le Collège d'Alma doit adopter, garder à jour et veiller à l'application d'une politique de sécurité de l'information (SI) pour assurer la mise en place des processus formels de la sécurité de l'information afin d'encadrer la gestion des risques, la gestion des accès aux actifs informationnels, la gestion des incidents et la gestion de la continuité des activités.

1. DÉFINITIONS

Dans la présente Politique, à moins que le contexte ne s'y oppose, les mots suivants sont définis comme suit :

a) Actif informationnel

Information ou donnée représentant de la valeur pour le Collège, soit :

- Une banque d'informations, sur quelque support qu'elle se trouve, incluant le papier ;
- Tous les types de documents produits ou reçus ;
- Les données transitant sur les systèmes d'information, y compris les logiciels ;
- Un réseau de télécommunication ou système de transmission de l'information tel que le courriel ;
- Une infrastructure technologique ou un ensemble de ces éléments (ordinateur, serveur, portable, disque externe, clé USB, appareil de télécommunication, etc.).

b) Catégorisation de l'information

Action de regrouper des données ou des informations, tangibles ou numériques, permettant de déterminer le niveau de criticité des actifs informationnels, ceci en tenant compte de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité de ces actifs.

c) Autorisation

Attribution par une autorité de droits d'accès aux Actifs informationnels qui consiste en un privilège d'accès accordé à une personne, à un dispositif ou à une entité.

d) Renseignements personnels

Tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier, tel que : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, l'occupation, le numéro d'assurance sociale, la date de naissance, la photographie et les coordonnées bancaires. Les Renseignements personnels doivent être protégés, peu importe la nature de leur support et quelle que soit leur forme : écrite, graphique, sonore, visuelle, informatisée ou autre.

e) Personne utilisatrice des actifs informationnels

Tout membre du personnel et toute personne physique ou morale qui utilise les actifs informationnels du Cégep.

f) Risque de sécurité de l'information

Tout événement lors du traitement, l'utilisation ou l'entreposage comportant un degré d'incertitude, qui pourrait porter atteinte à la confidentialité, l'intégrité et la disponibilité de l'information et causer un préjudice.

g) Détenteurs de l'information :

Les détentrices et détenteurs de l'information sont responsables d'assurer la sécurité d'un ou de plusieurs actifs informationnels qui leur sont confiés par la Direction générale de l'organisation. Ce rôle est attribué à un cadre de chaque direction ou direction adjointe. Les tâches quotidiennes peuvent être confiées à des détenteurs de l'information délégués.

2. OBJECTIFS DE LA POLITIQUE

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 son support ou ses moyens de communication. Plus précisément le Collège doit veiller à :

- La disponibilité de l'information de façon 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 de cette information lui procure 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, surtout si elle constitue des renseignements personnels.

3. CADRE LÉGAL ET ADMINISTRATIF

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

- La Directive gouvernementale sur la sécurité de l'information;
  Directive gouvernementale sur la sécurité de l'information

- Cadre gouvernemental de gestion de la sécurité de l'information
  Cadre gouvernemental de gestion de la sécurité de l'information

- Aide-mémoire : Politique gouvernementale en cybersécurité
  Politique gouvernementale en Cybersécurité - Mesures Clés

- La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1);
  Loi concernant le cadre juridique des technologies de l'information

- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1);
  Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25);
  Aide-Mémoire: Modernisation de la protection des renseignements personnels | Gouvernement du Québec

- Règlement sur les incidents de confidentialité
  Règlement sur les incidents de confidentialité

POLITIQUES DU COLLÈGE D'ALMA

- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03);
  Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement

- Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la *Loi sur la gouvernance et la gestion des ressources informationnelles*;
  Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la LGGRI

- Règles relatives à la gestion des projets en ressources informationnelles;
  Règles relatives à la gestion des projets en ressources informationnelles

- Règles relatives à la planification et à la gestion des ressources informationnelles;
  Règles relatives à la planification et à la gestion des ressources informationnelles

- La *Loi sur les archives* (LRQ, chapitre A-21.1);
  Loi sur les archives

- Les lois sectorielles régissant la mission de chaque organisme;

- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;

- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2);

  Règlement sur la diffusion de l'information et sur la protection des renseignements personnels

- La Charte des droits et libertés de la personne (LRQ, chapitre C-12);
  Charte des droits et libertés de la personne

- Le Code civil du Québec (LQ, 1991, chapitre 64);
  Code civil du Québec

- Le Code criminel (LRC, 1985, chapitre C-46);
  Code criminel

- Loi sur la fonction publique (RLRQ, chapitre F-3.1.1);
  Loi sur la fonction publique

- La Politique relative à l'emploi et à la qualité de la langue française du Collège;
- La Politique pour un collège sans violence ni harcèlement;
- Le Règlement relatif aux conditions de vie au Collège;
- Les conventions collectives en vigueur au Collège ;
- Toute autre loi ou règle applicable.

4. CHAMPS D'APPLICATION

a) Personnes visées

Cette politique vise sans exception l'ensemble des personnes physiques et morales, régulières ou occasionnelles, peu importe leur statut, appelées à utiliser les Actifs informationnels du Collège, dont notamment :

- Le personnel à l'emploi du Collège ;
- Les étudiantes et étudiants du Collège ;
- Les partenaires, fournisseurs, contractants et tiers du Collège.

b) Actifs visés

La Politique vise toutes les informations et les Actifs informationnels :

- Appartenant au Collège ;
- Détenus par un tiers, mais appartenant au Collège ;
- Utilisés et détenus par un tiers au bénéfice ou au nom du Collège ;

Et ce, qu'importe le support de conservation (électronique, technologique, papier, etc.).

c) Activités visées

Cette Politique concerne l'ensemble du Cycle de vie de l'information, à savoir : *la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation et la destruction des Actifs informationnels du Collège, qu'ils soient utilisés dans le périmètre de ses locaux, dans un autre endroit ou à distance.*

5. PRINCIPES GÉNÉRAUX

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

- s'appuyer sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires;

- s’assurer de bien connaître les actifs informationnels du Collège, en définir les caractéristiques de sécurité et en établir les responsables;

- protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;

- partager les meilleures pratiques et partager de l’information opérationnelle en matière de la sécurité de l’information avec le réseau de l’éducation et les organismes publics;

- assurer la régulation des conduites et la responsabilisation individuelle (chaque individu qui a accès à l’information étant responsable de respecter les critères de confidentialité, de disponibilité et d’intégrité de celle-ci);

- adhérer à une approche basée sur le risque acceptable, par une combinaison de mesures raisonnables, proportionnelles aux conséquences potentielles d’un bris de sécurité;

- mettre en place des mesures proactives de sécurité, des méthodes de détection d’usage inapproprié de l’information et des actions d’éradication des menaces;

- reconnaître que les actifs informationnels du Collège soutiennent ses activités professionnelles et pédagogiques et que les utilisatrices et utilisateurs en font usage à ces fins;

- reconnaître que tout actif informationnel mis à la disposition d’une utilisatrice ou d’un utilisateur est la propriété exclusive du Collège et non d’un département ou d’un service;

6. CADRE DE GESTION DE LA SÉCURITÉ DE L’INFORMATION

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

La politique de sécurité de l’information du Collège se base sur les axes fondamentaux de gestion suivants :

a) Gestion des identités et des accès (GIA)

Dans le but de protéger la confidentialité de l’information, la GIA est encadrée et contrôlée pour faire en sorte que l’accès, la divulgation et l’utilisation de toute information détenue par le Collège soient strictement réservés aux personnes autorisées.

b) Gestion des vulnérabilités

La gestion des vulnérabilités se caractérise par un déploiement des mesures pour maintenir à jour les logiciels du parc informatique, afin de garder les vulnérabilités au niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une gestion de notification des vulnérabilités venant des fournisseurs ou des prestataires de services doit être en place pour qu'elles soient évaluées et corrigées, le cas échéant.

c) Gestion du risque

La gestion des risques touchant les actifs informationnels du Collège est basée sur une analyse des menaces encourues reliées à l'intégrité, la disponibilité et la confidentialité de l'information détenue par le Collège. De cette analyse découlent des directives reliées à l'utilisation et l'opération des systèmes d'information ainsi qu'aux résultats escomptés.

d) Gestion des incidents

La gestion des incidents se caractérise par la mise en place de procédures de compte rendu, d'analyse relativement aux incidents de sécurité et de mesures correctives pour y donner suite. Les mesures déployées visent à assurer la continuité des services. Dans la gestion des incidents, le Collège peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'actif informationnel.

e) Gestion de la reprise et de la continuité des affaires

Elle se caractérise par la mise en place des processus pour identifier les incidents opérationnels majeurs susceptibles de menacer l'institution financière tels les catastrophes naturelles, les pannes d'électricité ou de télécommunication, les pannes informatiques, le piratage, le terrorisme, les pandémies, etc. L'identification de ces incidents permet d'évaluer leurs impacts sur les activités de l'institution et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

7. RÔLES ET RESPONSABILITÉS

a) Conseil d'administration (CA)

Le conseil d'administration adopte la *Politique sur la sécurité de l'information* ainsi que toute modification à celle-ci. Le conseil est informé des actions du Collège en matière de sécurité de l'information à travers le processus de plan d'action institutionnel.

b) Comité de direction (CD)

Le comité de direction du Collège détermine des mesures visant à favoriser l'application de la politique et des obligations légales du Collège en matière de sécurité de l'information. Ainsi, il propose les orientations ainsi que les plans d'action et il effectue les bilans de sécurité de l'information. Il peut également déterminer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

c) Direction générale (DG)

- S'assurer du respect et de la mise en œuvre de la présente Politique ;
- Nommer le chef de la sécurité de l'information organisationnelle (ci-après le « *CSIO* ») et le coordonnateur organisationnel des mesures de sécurité de l'information (ci-après le « *COMSI* »).

d) Chef de la sécurité de l'information organisationnelle (CSIO)

- Assumer la responsabilité de la prise en charge globale de la sécurité de l'information au Collège ;
- S'assurer de la diffusion et de la mise en application de la Politique, considérant la délégation de la part de la direction générale ;
- Proposer au Collège les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité ainsi que les redditions de comptes en matière de sécurité de l'information. ;
- Procéder, une (1) fois par année, à une reddition de comptes en matière de sécurité de l'information auprès du CA.

e) Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

- Intervenir dans la mise en œuvre des mesures et apporter le soutien nécessaire au CSIO du Collège, notamment en matière de la gestion des incidents et des Risques en sécurité de l'information;
- Représenter le Collège auprès du Réseau d'alerte gouvernemental;
- S'assurer de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) ;
- Contribuer aux analyses de Risques en sécurité de l'information ;
- Contribuer au processus formel de gestion des droits d'accès à l'information.

f) Détentrices et détenteurs de l'information

Ils doivent :

- déterminer les règles d'accès et approuver les demandes d'accès des utilisatrices et utilisateurs;
- évaluer le risque de leurs actifs et s'assurer que les mesures de sécurité appropriées soient élaborées, approuvées, mises en place et appliquées systématiquement;
- adopter le plan de continuité en cas de panne;
- s'assurer que tous les employées et employés de leur service sont au fait de leurs obligations en matière de sécurité.

g) Direction des technologies de l'information (DTI)

En matière de sécurité de l'information, la Direction des technologies de l'information 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.

En ce sens :

- Elle accompagne les gestionnaires du Collège dans la mise en application de la présente Politique ;
- Elle assure la sécurité des technologies de l'information en déployant les mesures nécessaires et appropriées ;
- Elle élabore et met en œuvre des activités de sensibilisation à la sécurité de l'information pour les membres du personnel et les membres de la communauté étudiante du Collège en collaboration avec la Direction des ressources humaines et des affaires corporatives (DRHAC) et la Direction des études ;
- Elle applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, tel que par exemple l'interruption ou la révocation temporaire - lorsque les circonstances l'exigent - des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause;
- Elle participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique et autorisées par la Direction générale.

h) Direction des services administratifs (DSA)

La Direction des services administratifs participe, avec le Responsable de la sécurité de l'information, à l'établissement des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Collège.

i) Direction des ressources humaines et des affaires corporatives (DRHAC)

En matière de sécurité de l'information, la Direction des ressources humaines :

- obtient de tout nouveau membre du personnel du Collège, après lui en avoir montré la nécessité, son engagement au respect de la politique;
- informe les détentrices et détenteurs de l'information et la Direction des technologies de l'information des changements de statut du personnel;

j) Utilisatrices et utilisateurs

Toute utilisatrice ou tout utilisateur qui accède à une information du Collège, 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, cette personne 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 détenteur de l'information 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;

Aussi, toute utilisatrice ou tout utilisateur du Collège doit se conformer aux politiques et aux directives en vigueur 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. FORMATION, SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur l'adoption des comportements sécuritaires et sur la responsabilisation individuelle.

À cet égard, le personnel ainsi que les étudiantes et les étudiants doivent être sensibilisés :

- À la sécurité de l'information et des systèmes d'information du Collège;
- Aux conséquences d'une atteinte à la sécurité ;
- À leurs rôles et à leurs responsabilités en la matière.

Le Collège s'engage sur une base régulière à sensibiliser et à former les utilisatrices et les utilisateurs à la sécurité des Actifs informationnels, aux conséquences d'une atteinte à la sécurité de ces Actifs ainsi qu'à leur rôle et leurs obligations en la matière. Les utilisatrices et les utilisateurs ont la responsabilité de participer à ces activités de sensibilisation et de formation.

9. SANCTIONS

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

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 une suspension de ses droits d'accès aux actifs informationnels. Il s'expose aussi à d'autres sanctions, selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles disciplinaires internes applicables.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, une ou un partenaire, une invitée ou un invité, une consultante ou 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.

10. DISPOSITIONS GÉNÉRALES

La Direction générale est responsable de la sécurité de l'information et elle est responsable de la diffusion et de la mise à jour de cette politique. Nonobstant ce qui précède, cette dernière peut déléguer cette responsabilité à la personne CSIO et à la Direction des technologies de l'information .

Cette politique entre en vigueur dès son adoption par le conseil d'administration du Collège. Elle et remplace toute politique antérieure.

Sa révision et sa mise à jour doivent être effectuées au plus tard aux cinq ans.

Cette révision remplace la précédente ADM-20 adoptée le 26 avril 2021.