Collège de Maisonneuve

# POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Adoptée le : 7 juin 2019
Lors de la : 328e réunion du conseil d'administration

Modifiée le : 18 septembre 2023
Lors de la : 351e réunion du conseil d'administration

# TABLE DES MATIÈRES

## PRÉAMBULE

Le Collège de Maisonneuve (ci-après le « Collège ») 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. Vu la valeur administrative, légale et financière de ses Actifs informationnels, le Collège se doit d'en faire une évaluation continue. Il se doit également d'en assurer une utilisation et une protection appropriées et adéquates tout au long de leur Cycle de vie, selon les bonnes pratiques en matière de sécurité informationnelle en intégrant une approche de gestion des risques, et ce, 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 impose des obligations importantes aux établissements collégiaux.

Pour se conformer et répondre à ses obligations réglementaires et légales, le Collège doit adopter, garder à jour et mettre en application la présente *Politique de sécurité de l'information* (ci-après la « Politique »).

## 1. DÉFINITIONS

Dans la présente Politique, à moins que le contexte ne s'y oppose, les expressions suivantes signifient :

### 1.1 Actif informationnel

Information numérique, document numérique, système d'information, documentation, équipement informatique, technologie de l'information, installation ou ensemble de ces éléments, acquis ou constitué par le Collège pour mener à bien sa mission.

### 1.2 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.

### 1.3 Cadre de gestion

Ensemble de consignes que sont les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues qui encadrent les activités d'un établissement, tel qu'un cégep.

### 1.4 Code d'accès

Mécanisme d'identification et d'authentification par un code individuel et un mot de passe ou de ce qui en tient lieu, notamment une carte magnétique ou carte à puce, servant à identifier de façon unique un utilisateur qui utilise un Actif informationnel du Collège.

### 1.5 Confidentialité

Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées.

### 1.6 Cycle de vie de l'information

Ensemble des étapes que parcourt une information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du Collège.

### 1.7 Disponibilité

Propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

### 1.8 Équipement informatique

Ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communication, de réception et de traitement de l'information, et tout équipement de télécommunications.

### 1.9 Gestionnaire

Personne-cadre détenant l'autorité au sein d'un service ou d'une direction, qu'elle soit d'ordre pédagogique ou d'ordre administratif.

### 1.10 Intégrité

Propriété d'une information ou d'une technologie de l'information de n'être ni modifiées, ni altérées, ni détruites sans Autorisation.

### 1.11 Plan de relève informatique

Ensemble de procédures qui décrivent de façon précise les mesures à suivre pour remettre en état de fonctionnement un système informatique à la suite d'une panne ou d'un sinistre majeur.

### 1.12 Risques liés à la sécurité de l'information

Tout événement lors du traitement, de l'utilisation ou de 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.

### 1.13 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.

### 1.14 Technologies de l'information

Regroupent les techniques, principalement de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie) qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre de l'information.

## 2. CHAMP D'APPLICATION

### 2.1 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.

### 2.2 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.).

### 2.3 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.

## 3. OBJECTIFS DE LA POLITIQUE

La présente Politique constitue le cadre général qui vise la gestion des Actifs informationnels dans le respect des droits et des obligations du Collège en cette matière pour garantir et répondre aux objectifs de sécurité de l'information et plus spécifiquement pour :

- Assurer la protection de l'Actif informationnel tout en long de son Cycle de vie, quel que soit le support ou l'emplacement;
- Assurer la Disponibilité de l'information pour qu'elle soit accessible au moment voulu et utilisable à la demande de l'entité autorisée;
- Assurer l'Intégrité de l'information en la préservant contre toute destruction, modification et altération de quelque façon que ce soit sans Autorisation;

- Préserver la Confidentialité de l'information en s'assurant de ne pas la rendre accessible ou de ne pas la divulguer à des personnes, entités ou processus non autorisés;
- Regrouper les lignes directrices et les rôles et responsabilités des différents intervenants en sécurité de l'information;
- Identifier et classifier les Actifs informationnels du Collège selon leurs degrés de criticités et veiller à leur évaluation constante ainsi qu'à leur protection adéquate;
- Assurer la conformité du Collège aux lois et aux règlements;
- Mettre en place un plan de continuité des activités et de relève informatique;
- Assurer le respect de la vie privée des personnes physiques, notamment la Confidentialité de leurs Renseignements personnels.

## 4. CADRE LÉGAL ET NORMATIF

- 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

- 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

- 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

- Toute autre loi ou règle applicable;

- Le Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information;

- Le cadre gouvernemental de gestion de la sécurité de l'information;

- Les normes internationales, notamment ISO 27000 et NIST 800-60;

- Les pratiques gouvernementales en matière de sécurité de l'information.

## 5. ÉNONCÉ DES PRINCIPES GÉNÉRAUX

### 5.1 Protection de l'information

La sécurité de l'information s'articule autour des trois principes suivants :

1) Disponibilité

   La Disponibilité garantit que les utilisateurs autorisés d'un système ont un accès opportun et ininterrompu aux informations contenues dans ce système ainsi qu'au réseau. Les informations doivent être accessibles en temps utile et de la manière

requise par un utilisateur autorisé. Afin d'aider à assurer cette Disponibilité, des mesures de contrôles doivent être mises en place.

2) Intégrité

   L'Intégrité des données consiste à garantir que les données n'ont pas été modifiées d'aucune façon au cours de leur communication, qu'il s'agisse de données au repos, en transit ou en mémoire. Afin d'assurer l'Intégrité des données, des mesures de sécurité physiques et d'accès logiques doivent être mises en place.

3) Confidentialité

   La Confidentialité vise à empêcher tout accès non autorisé à des informations sensibles. Elle a pour but de s'assurer qu'une information ou une donnée soit accessible uniquement par les personnes autorisées. La Confidentialité de l'information doit aussi être assurée tout au long de son Cycle de vie. Afin de garantir la Confidentialité, des mesures de contrôle doivent être mises en place.

### 5.2 Catégorisation de l'information

L'information constitue une ressource essentielle qui doit être protégée tout au long de son Cycle de vie. Pour cette raison il est primordial de garder à jour l'inventaire de l'ensemble des Actifs informationnels de l'organisation. L'un des premiers intrants de la sécurité de l'information est la connaissance de la sensibilité de l'information des Actifs informationnels d'une organisation. La catégorisation des Actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des Actifs que dans le but d'en déterminer le niveau de protection.

Il est important de réévaluer la catégorisation des Actifs informationnels sur une base périodique pour s'assurer que la catégorisation attribuée est toujours appropriée en fonction des modifications des obligations légales et contractuelles ainsi que des changements dans l'utilisation des données ou leur valeur pour l'établissement. Cette évaluation doit être effectuée par le Gestionnaire, détenteur de l'Actif.

## 6. CADRE DE GESTION

La mise en œuvre de la présente Politique s'appuie sur la définition d'un Cadre de gestion en sécurité de l'information qui précise le champ d'action des différents intervenants. Le Cadre de gestion précise l'organisation fonctionnelle en matière de sécurité de l'information et rend possibles la définition d'objectifs clairs et une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information sont réévaluées 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 risques et des menaces.

La présente Politique se base sur cinq axes fondamentaux de gestion.

### 6.1 Gestion des identités et des accès (GIA)

La gestion des identités et des accès 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 afin de protéger la Confidentialité.

### 6.2 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.

### 6.3 Gestion des Risques

La gestion des Risques touchant l'Actif informationnel 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.

### 6.4 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.

### 6.5 Gestion de la reprise et de la continuité des affaires

La gestion de la reprise et de la continuité des affaires se caractérise par la mise en place des processus pour identifier les incidents opérationnels majeurs susceptibles de menacer le Collège, 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 du Collège et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

## 7. RÔLES ET RESPONSABILITÉS

La présente Politique attribue la gestion de la sécurité de l'information du Collège à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

### 7.1 Conseil d'administration

- Adopter la présente Politique.

### 7.2 Direction générale

- 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 »).

## 7.3 Responsable de l'accès à l'information et de la protection des renseignements personnels[1]

- Chapeauter l'ensemble des activités du comité sur l'accès à l'information et la protection des renseignements personnels;
- Tenir un registre de communications des Renseignements personnels;
- Traiter les demandes d'accès à des Renseignements personnels;
- Traiter les demandes de rectification à un fichier contenant des Renseignements personnels;
- S'assurer du suivi des incidents de confidentialité;
- Traiter les plaintes relatives aux incidents de confidentialité;
- S'assurer de la mise à jour de la *Politique relative à la protection des renseignements personnels*;
- S'assurer de la diffusion et de la mise à jour de la *Politique relative à la protection des renseignements personnels* sur le site Web du Collège;
- S'assurer de l'application de la *Politique relative à la protection des renseignements personnels*.

## 7.4 Chef de la sécurité de l'information organisationnelle (CSIO)[1]

- 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.

## 7.5 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)[1]

- 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);
- Soutenir le CSIO;
- Collaborer, auprès du CSIO, à l'élaboration des divers éléments stratégiques et tactiques en sécurité informationnelle :
    - ❖ Maintenir le registre des événements et des incidents liés à la sécurité de l'information;
    - ❖ Effectuer et participer aux analyses de Risques en sécurité de l'information;

[1] L'annexe à la présente Politique établit l'identité des personnes assumant ces rôles au sein du Collège.

- ❖ Gérer le processus de gestion, de déclaration des incidents et de résolution de problème et contribuer à sa mise en place;
- ❖ Contribuer au processus formel de gestion des droits d'accès à l'information.

## 7.6 Direction des ressources informationnelles

- Promouvoir l'application de la présente Politique;
- S'assurer de la prise en charge des exigences de la 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;
- Participer, avec le CSIO, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les Actifs informationnels du Collège, afin d'intégrer des mesures de protection en fonction du niveau de sensibilité de l'information, en tenant compte des exigences réglementaires, d'affaires, légales ou contractuelles.

## 7.7 Direction des ressources humaines

- Vérifier, au besoin, les antécédents des candidats à l'embauche et des membres du personnel du Collège impliqués dans la sécurité de l'information;
- Informer et obtenir de tout nouveau membre du personnel du Collège son engagement au respect de la présente Politique;
- Imposer les sanctions appropriées lors de violation des politiques, règlements, directives et code de conduite touchant à la sécurité de l'information.

## 7.8 Gestionnaire

- Assumer le rôle de responsable des Actifs, papiers ou informationnels, comportant ou non des Renseignements personnels, qu'il détient;
- Participer à la catégorisation de l'information de l'unité sous sa responsabilité et à l'analyse de Risques;
- Veiller à la protection de l'information et des systèmes d'information en conformité avec la présente Politique;
- Rapporter tout événement ou toute menace liée à la sécurité de l'information;
- Collaborer à la mise en œuvre de toute mesure pour améliorer la sécurité de l'information afin de remédier à un incident au besoin.

## 7.9 Personnel du Collège

- 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;
- Être responsable des actions résultant de l'usage de son identifiant, de son Code d'accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers, à moins qu'il démontre que les actions posées par un tiers ne découlent pas d'une négligence ou d'une malveillance de sa part;

- Aviser son Gestionnaire de toute situation susceptible de compromettre la sécurité de l'Actif informationnel;
- Au besoin, participer à la catégorisation de l'information de son service;
- 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 approprié à son utilisation et aux fins auxquelles ils sont destinés;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- 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.

### 7.10 Étudiante ou étudiant

- 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;
- Être responsable des actions résultant de l'usage de son identifiant, de son Code d'accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers, à moins qu'il démontre que les actions posées par un tiers ne découlent pas d'une négligence ou d'une malveillance de sa part;
- Aviser un de ses enseignants de toute situation susceptible de compromettre la sécurité de l'Actif informationnel;
- 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 approprié à son utilisation et aux fins auxquelles ils sont destinés;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- 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.

## 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 ne soit pas protégée adéquatement.

Le membre du personnel, l'étudiante ou l'étudiant 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 administratives ou disciplinaires internes applicables ou du contrat en vigueur.

## 10. RÉVISION DE LA POLITIQUE

La Politique sera révisée au besoin, ou au minimum, tous les 5 ans à compter de sa date d'adoption.

## 11. ENTRÉE EN VIGUEUR

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

Le conseil d'administration délègue au comité de direction l'adoption de toute modification de l'annexe à la présente Politique.

## ANNEXE

| | |
|---|---|
| **Responsable de l'accès à l'information et de la protection des renseignements personnels** | Mme Karolyne Gagnon, directrice des affaires juridiques et secrétaire générale |
| **Chef de la sécurité de l'information organisationnelle (CSIO)** | M. Éric Raymond, directeur des ressources informationnelles |
| **Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)** | Mme Lila Ouchia, directrice adjointe des ressources informationnelles<br><br>M. François Jacques, analyste en sécurité informatique |