CHAMPLAIN
REGIONAL COLLEGE

Politique de sécurité de l'information

Champlain
COLLEGE LENNOXVILLE

1958

St.Lawrence
CEGEP CHAMPLAIN

Champlain
COLLEGE SAINT-LAMBERT

Historique des adoptions et révisions

Recontre du conseil d'administration	Numéro de résolution	Notes
14 juin 2024	CRC-2023-065	

Table des matières

1. Préambule

Le Collège régional de Champlain (le « Collège ») reconnaît que l'information et les technologies qui la soutiennent sont essentielles à son fonctionnement quotidien et à la réalisation de sa mission d'enseignement et de recherche. Compte tenu de la valeur administrative, juridique et financière de ses actifs informationnels, ceux-ci 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, conformément aux meilleures pratiques en matière de sécurité de l'information et à une approche de gestion des risques, quel que 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 (L.R.Q., c. G-1.03), de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (L.R.Q., 2021, c. 25) et de la Directive gouvernementale sur la sécurité de l'information (2021), émise par le Secrétariat du Conseil du trésor du Québec et applicable aux organismes publics, impose des obligations importantes aux collèges.

Afin de se conformer à ses obligations réglementaires et légales, le Collège doit adopter, maintenir et appliquer une politique de sécurité de l'information (la « Politique ») garantissant la mise en œuvre de processus formels pour la gestion des risques, l'accès aux actifs informationnels, les incidents et la continuité des activités.

2. Objectifs

La Politique fournit le cadre général pour la gestion des actifs informationnels conformément aux droits et responsabilités du Collège en la matière afin d'assurer et d'atteindre les normes de sécurité de l'information et plus particulièrement pour :

- Garantir la protection des actifs informationnels tout au long de leur cycle de vie, quel que soit leur support ou leur emplacement ;
- Veiller à ce que les informations soient disponibles lorsqu'elles sont nécessaires et puissent être utilisées par les personnes autorisées lorsqu'elles en ont besoin ;
- Garantir l'intégrité des informations en les protégeant contre toute destruction, modification ou altération non autorisée ;
- Préserver la confidentialité des informations en veillant à ce qu'elles ne soient pas mises à la disposition ou divulguées à des personnes, entités ou processus non autorisés ;
- Consolider les lignes directrices ainsi que les rôles et responsabilités des parties prenantes en matière de sécurité ;
- Identifier et classer les actifs informationnels du Collège en fonction de leur niveau de criticité, puis veiller à ce qu'ils soient continuellement évalués et protégés de manière adéquate ;
- Veiller au respect des lois et réglementations applicables ;
- Assurer la continuité organisationnelle en mettant en œuvre un plan de reprise après sinistre informatique ;

- Veiller au respect de la vie privée des individus, y compris de la confidentialité des informations personnelles.

3. Cadre juridique et réglementaire

Outre le cadre de gestion de la sécurité de l'information du Collège et les documents connexes, le Collège doit se conformer aux lois, règlements, normes et pratiques gouvernementales en vigueur.

La politique existe et repose sur ces fondements juridiques et réglementaires. Elle est régie par :

- La directive gouvernementale sur la sécurité de l'information
- Le cadre gouvernemental de gestion de la sécurité de l'information
- Mesures clés : Politique gouvernementale en matière de cybersécurité
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., 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)
- Règlement sur les incidents de confidentialité (LRQ, chapitre A-2.1, r. 3.1)
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03)
- 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 des organismes publics et des entreprises du gouvernement (LRQ, c. G-1.03, r. 1)
- Règles relatives à la gestion des projets liés aux ressources informationnelles (Décret 1159-2022)
- Règles relatives à la planification et à la gestion des ressources informationnelles (A.M. 2022-03)
- Loi sur les archives (LRQ, c. A-21.1)
- Loi sur le droit d'auteur (L.R.C. (1985), ch. C-42)
- Cadre stratégique pour la gouvernance et la gestion des ressources documentaires des organismes publics.
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (LRQ, c. A-2.1, r 2)
- Charte des droits et libertés de la personne (LRQ, c. C-12)
- Code civil du Québec (LQ, 1991, c. 64)
- Code criminel (L.R.C. (1985), ch. C-46)
- Loi sur la fonction publique (RLRQ, c. F-3.1.1)
- Cadre de gestion des risques et des incidents à portée gouvernementale
- Normes internationales, notamment ISO 27000, NIST 800-60 et COBIT
- Exigences du *Ministère de la Cybersécurité et du Numérique (MCN)* et des *Centres opérationnels de cyberdéfense (COCD)*

- Tous les règlements, politiques et directives du Collège
- Toute autre loi ou réglementation applicable.

4. Portée

4.1. Public visé

Cette politique s'applique sans exception à toutes les personnes et entités, régulières ou occasionnelles, quel que soit leur statut, qui sont appelées à utiliser les ressources d'information du Collège :

- Les employés du Collège ;
- Les étudiants du Collège ;
- Les invités, partenaires, fournisseurs, sous-traitants et tiers du Collège.

4.2. Actifs visés

La politique couvre également toutes les informations et tous les actifs informationnels, quel que soit leur support de stockage (électronique, technologique, papier, etc.) qui appartiennent au Collège, qu'ils soient :

- détenus par le Collège lui-même ; ou
- détenus et/ou utilisés par un tiers pour le compte du Collège.

4.3. Activités visées

Cette politique s'applique à l'ensemble des activités liées au cycle de vie de l'information, c'est-à-dire à la collecte, à l'enregistrement, au traitement, à la modification, à la diffusion, à la conservation et à la destruction des actifs informationnels du Collège, qu'elles soient effectuées dans les locaux du Collège, à d'autres endroits ou à distance.

5. Définitions

Actif informationnel : toute information ou document numérique, tout système d'information, toute documentation, tout équipement informatique, toute technologie de l'information, toute installation ou tout ensemble de ces éléments acquis ou créés par le Collège pour mener à bien sa mission.

Autorisation : octroi de droits d'accès aux actifs informationnels par une autorité, consistant en un privilège d'accès accordé à une personne, un appareil ou une entité.

Cadre de gestion : ensemble d'instructions sous forme de politiques, de règlements, de directives, de procédures, de bonnes pratiques reconnues et de normes industrielles qui régissent les activités d'une organisation telle qu'un établissement d'enseignement supérieur.

Catégorisation : processus consistant à déterminer le degré de sensibilité des actifs informationnels du Collège, en tenant compte de l'impact qu'une atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité pourrait avoir.

CERT/QC : acronyme désignant l'équipe d'intervention en cas d'incident de sécurité informatique et le réseau d'alerte du gouvernement du Québec. *Computer Emergency Response Team/Québec*.

Code d'accès : mécanisme d'identification et d'authentification utilisant un code et un mot de passe individuels, ou un substitut tel qu'une carte magnétique, une carte à puce ou un jeton de sécurité, permettant d'identifier de manière unique un utilisateur accédant à une ressource informationnelle du Collège.

Le **Collège :** désigne le Collège régional Champlain dans son ensemble, qui offre des programmes d'enseignement général et professionnel, ainsi que ses collèges constituants.

Collège constituant : désigne les collèges constituants du Collège régional de Champlain dans lesquels les étudiants sont inscrits à des fins éducatives, à savoir Champlain College – Lennoxville, Champlain – St. Lawrence College et Champlain College – Saint-Lambert, individuellement ou collectivement selon le contexte.

Cycle de vie de l'information : ensemble des étapes par lesquelles passe une information depuis sa création, son enregistrement, son transfert, sa récupération, son traitement et sa transmission jusqu'à sa conservation ou sa destruction conformément au calendrier de conservation du Collège.

Document : ensemble d'informations véhiculées par un support. Les informations sont délimitées et structurées de manière tangible ou logique selon le support, et sont intelligibles sous forme de mots, de sons ou d'images. Les informations peuvent être représentées sous toute forme d'écriture, y compris un système de symboles transcrit dans l'une de ces formes ou dans un autre système de symboles. Une base de données est un document si ses éléments structurants permettent de créer des documents en délimitant et en structurant les informations qu'elle contient.

Équipement informatique : ordinateurs portables, mini-ordinateurs, micro-ordinateurs, postes de travail informatiques et leurs périphériques ou accessoires permettant de lire, stocker, reproduire, imprimer, transmettre, recevoir et traiter des informations, ainsi que tout équipement de télécommunication.

Garant : personne responsable de la sécurité d'un actif informationnel sous sa responsabilité.

Gestionnaire : autorité administrative au sein d'un département ou d'une unité, qu'elle soit pédagogique ou administrative.

Incident : événement affectant ou pouvant affecter la disponibilité, l'intégrité ou la confidentialité des informations, ou plus généralement la sécurité des systèmes d'information, comme une interruption ou une dégradation des services.

Logiciel : ensemble de programmes conçus pour effectuer une tâche spécifique sur un ordinateur. Le terme « logiciel » désigne tous les types de programmes, y compris les systèmes d'exploitation.

Membres de la communauté du Collège : désignent tous les étudiants, enseignants et employés du Champlain Regional College. Un étudiant qui est également employé est avant tout un étudiant. Pour les besoins de la présente politique, le terme désigne également les sous-traitants et les prestataires de services tiers, les invités des étudiants et des employés, les représentants syndicaux, les représentants des associations étudiantes, les bénévoles, les sponsors et les membres des organes de gouvernance du Collège.

Mesures de sécurité de l'information : moyens concrets permettant de protéger partiellement ou totalement les actifs informationnels du Collège contre un ou plusieurs risques (panne majeure du réseau informatique ou du serveur, acte involontaire, acte malveillant tel qu'une intrusion dans un système informatique, etc.) et dont la mise en œuvre vise à réduire la probabilité de survenue de ces risques ou à limiter les pertes qui en résultent.

Normes de sécurité de l'information : série de processus documentés qui définissent la manière de mettre en œuvre, de gérer et de surveiller divers contrôles de sécurité. Elles fournissent également un plan directeur permettant d'atténuer les risques et de réduire les vulnérabilités, ainsi que des normes et des cadres de cybersécurité pour se conformer à la réglementation. Ces normes comprennent notamment des lois, des règlements et des directives gouvernementales, ainsi que des normes internationales reconnues telles que ISO 27000, NIST 800-60, MITRE ATT&CK et COBIT.

Plan de continuité et de reprise des activités informatiques : ensemble de procédures détaillant les mesures à prendre pour rétablir un système informatique après une panne ou une catastrophe majeure.

Risque acceptable : capacité objective de l'organisation à poursuivre ses activités malgré la survenue d'un risque lié à la sécurité de l'information. Seuil de risque au-delà duquel les actifs informationnels sont exposés à un risque intolérable.

Risque lié à la sécurité de l'information : degré d'exposition d'une information ou d'un système d'information à une menace d'interruption ou de dégradation de la qualité du service, ou à une menace pour la disponibilité, l'intégrité ou la confidentialité de l'information, pouvant affecter la prestation de services, la vie, la santé ou le bien-être des personnes, la protection de leurs renseignements personnels, le respect de leur vie privée ou l'image du Collège.

Risques liés à la sécurité de l'information gouvernementale : risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale, ce qui pourrait nuire à la prestation de services au public, à la vie, à la santé ou au bien-être des personnes, au respect de leurs droits fondamentaux, à la protection de leurs renseignements personnels et de leur vie privée, à l'image du gouvernement ou à la prestation de services par d'autres organismes publics.

Technologies de l'information : technologies, principalement informatiques, audiovisuelles, multimédias, Internet et de télécommunication (réseaux câblés et sans fil et téléphonie), qui permettent aux utilisateurs de communiquer, d'accéder à des sources d'information, de stocker, de manipuler, de produire et de transmettre des informations.

Utilisateur : toute personne physique ou morale qui utilise ou a accès aux ressources informationnelles du Collège. Il s'agit notamment, mais pas uniquement, des enseignants, du personnel professionnel, du personnel de soutien, des gestionnaires, des étudiants, des syndicats ou associations qui les représentent, des locataires de logements étudiants et des prestataires de services tiers.

6. Rôles et responsabilités

La sécurité de l'information repose sur une approche éthique visant à réglementer les comportements et à garantir la responsabilité individuelle. Une sécurité de l'information efficace requiert une responsabilité clairement définie à tous les niveaux du collège.

La politique confie la gestion de la sécurité de l'information du Collège à diverses entités, comités et personnes, en fonction des fonctions qu'ils exercent.

6.1. Conseil d'administration

Le conseil d'administration approuve et adopte la politique, les principes directeurs ainsi que toute modification ultérieure. Il se voit également présenter des rapports sur la sécurité de l'information.

6.2. Directeur général

Le directeur général est la principale autorité en matière de sécurité de l'information. À ce titre, il veille au respect et à l'application des lois et règlements relatifs à la sécurité de l'information, à la mise en œuvre du cadre gouvernemental de sécurité de l'information et à l'application de la politique de gestion de la sécurité de l'information y afférente. Il est également chargé de déléguer les fonctions du chef de la sécurité de l'information organisationnelle (CSIO) et des coordonnateurs organisationnels des mesures en sécurité de l'information (COMSI).

Le directeur général doit également :

- soutenir le CSIO ;
- approuver les documents officiels relatifs à la reddition en matière de sécurité de l'information ;

- autoriser, à titre exceptionnel, une dérogation à toute disposition de la politique, des directives ou des procédures du Collège affectant directement ou indirectement la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement lié à la mission du Collège ;
- diriger le comité de crise sur la sécurité de l'information.

6.3. Directeur de collège constituant

Le directeur d'un collège constituant est l'autorité de ce collège en matière de sécurité de l'information, conformément à l'autorité qui lui a été déléguée par le directeur général. À ce titre, il veille au respect et à l'application des lois et règlements en la matière, ainsi qu'à l'application du cadre gouvernemental et de la politique de gestion de la sécurité de l'information de son collège constituant.

Le directeur du collège constituant doit également :

- soutenir le directeur général dans son rôle d'autorité principale en matière de sécurité de l'information ;
- soutenir le CSIO ;
- participer au comité de crise sur la sécurité de l'information.

6.4. Affaires corporatives

Le service des affaires corporatives est chargé de veiller au respect et à l'application de la législation en matière d'archives, d'accès à l'information et de protection des renseignements personnels, ainsi que de mettre en œuvre les politiques et pratiques régissant cette protection.

À ce titre, les affaires corporatives doivent collaborer avec le CSIO pour :

- communiquer au CSIO les problèmes et les préoccupations en matière de sécurité concernant la protection des renseignements personnels ou sensibles ;
- assurer la cohérence et l'harmonisation entre la sécurité de l'information, l'accès aux documents et la protection de la vie privée, y compris la mise en œuvre de processus de gestion des risques et des incidents liés à la sécurité de l'information ;
- veiller à ce que le comité permanent sur la protection des renseignements personnels soit consulté pour mener une évaluation des facteurs relatifs à la vie privée (EFVP) pour tout projet impliquant l'acquisition, le développement ou la refonte d'un système d'information impliquant la collecte, l'utilisation, la divulgation, la conservation ou la destruction de renseignements personnels ;
- travailler en étroite collaboration avec les gestionnaires et le CSIO pour identifier, gérer, coordonner et mettre en œuvre des mesures de sécurité de l'information, quel que soit le support.

6.5. Chef de la sécurité de l'information organisationnelle (CSIO)

- Le CSIO est membre du personnel cadre du Collège ;
- La fonction de CSIO est déléguée par le directeur général ;
- Le CSIO relève du directeur général dans le cadre de la gestion de la sécurité de l'information du gouvernement ;
- Le CSIO est responsable de la gestion globale de la sécurité de l'information au sein de son organisation. Il travaille en étroite collaboration avec les parties prenantes gouvernementales concernées pour garantir le respect des exigences en matière de sécurité de l'information ;
- Le CSIO propose au Collège des orientations stratégiques, des évaluations des risques, des plans d'action, des évaluations de la sécurité et des rapports sur les questions de sécurité de l'information ;
- Le CSIO est responsable de la diffusion et de la mise en œuvre de la Politique.

6.6. Coordonnateur organisationnel des mesures en sécurité de l'information (COMSI)

Le COMSI intervient au niveau opérationnel. Il participe à la mise en œuvre des mesures et apporte le soutien nécessaire au CSIO, notamment en ce qui concerne la gestion des incidents et des risques liés à la sécurité de l'information.

Le COMSI représente également le Collège au sein du Réseau d'alerte gouvernemental (CERT/QC). Il est chargé d'appliquer le processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) pour le compte du Collège, en collaboration avec le CSIO.

Le COMSI appliquera les mesures d'intervention appropriées à toute menace ou tout incident lié à la sécurité de l'information, telles que l'interruption temporaire ou le retrait de l'accès et/ou des services à un système d'information, si les circonstances l'exigent, afin d'assurer la sécurité des informations concernées.

Il travaille avec le CSIO du Collège pour développer divers éléments stratégiques et tactiques en matière de sécurité de l'information :

- Il tient à jour un registre des événements et incidents liés à la sécurité de l'information ;
- Il mène et participe à l'analyse des risques liés à la sécurité de l'information ;
- Il gère et contribue à la mise en œuvre du processus de gestion des incidents, de signalement et de résolution ;
- Il contribue au processus officiel de gestion des identités et des accès (GIA).

6.7. Services des technologies de l'information

Les services des technologies de l'information sont responsables de l'application de la Politique dans leur établissement. Ils veillent à ce que les exigences en matière de sécurité de l'information soient prises en compte lors de l'exploitation des systèmes et des infrastructures informatiques, ainsi que lors de la mise en œuvre de projets de développement ou d'acquisition de systèmes informatiques.

Les services des technologies de l'information participent, avec le CSIO, à l'identification des mesures de sécurité visant à protéger de manière adéquate les actifs informationnels du Collège. Ces mesures sont intégrées en fonction du niveau de sensibilité des informations, tout en tenant compte des exigences réglementaires, organisationnelles, juridiques ou contractuelles.

Les services des technologies de l'information aident le CSIO et le COMSI à gérer, mettre en œuvre et rendre compte de toutes les questions liées à la sécurité de l'information telles que définies par les lois, les règlements et les cadres gouvernementaux.

Les services des technologies de l'information ont également pour mission :

- Veiller à l'application de la Politique ;
- Participer activement à l'analyse des risques, à l'évaluation des besoins et à la mise en œuvre des mesures de sécurité des systèmes d'information ;
- Collaborer avec le COMSI pour appliquer le processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) à leur collège ;
- Tenir un registre local de tous les incidents, menaces et vulnérabilités et les signaler immédiatement au COMSI ;
- Participer à la mise en œuvre de tous les mécanismes de sécurité de l'information nécessaires, tels que déterminés par la stratégie de sécurité de l'information du collège ;
- Participer aux enquêtes sur les violations réelles ou apparentes de la politique ;
- Effectuer et rendre compte des résultats de l'analyse des risques requise avant tous les projets informatiques.

6.8. Services des ressources humaines

En matière de sécurité de l'information, les services des ressources humaines doivent :

- Effectuer des vérifications des antécédents, le cas échéant, des candidats à l'emploi et du personnel chargé de la sécurité de l'information ;
- S'assurer que les descriptions de poste des employés incluent leurs responsabilités en matière de sécurité de l'information et de conformité à la politique et au cadre normatif relatif aux ressources informationnelles ;
- Informer tous les nouveaux employés du Collège et obtenir leur engagement à se conformer à la politique et au cadre de gestion associé ;

- Informer les services des technologies de l'information des embauches, des changements de poste et des licenciements afin de mettre à jour l'accès aux ressources informatiques du Collège conformément à la gestion des identités et des accès (GIA) ;
- Appliquer les sanctions appropriées en cas de violation des politiques, règlements, directives et codes de conduite en matière de sécurité de l'information.

6.9. Services des ressources matérielles

Les services des ressources matérielles, y compris les services liés aux bâtiments et aux équipements, travailleront avec le CSIO pour déterminer les mesures de sécurité physique nécessaires à la protection adéquate des actifs informationnels du Collège.

En matière de sécurité, les services des ressources matérielles doivent :

- Contrôler l'accès physique aux locaux du Collège ;
- Gérer l'accès physique (clés, cartes magnétiques, etc.) aux zones réglementées (salles informatiques, entrepôts, etc.) ;
- Conserver, dans un registre, les informations nécessaires pour suivre le niveau d'accès et les moyens d'accès du personnel au sein du Collège (attribution des clés, système de gestion des clés magnétiques, etc.).

6.10. Les gestionnaires

Les gestionnaires sont les garants des actifs informationnels dont ils ont la charge. Leur rôle consiste à veiller au respect des règles, des cadres, etc. applicables, afin de garantir l'accessibilité, une utilisation appropriée et la sécurité des actifs informationnels dont ils ont la charge. Ils peuvent déléguer tout ou partie de leurs responsabilités à une autre personne de leur service, sans pour autant renoncer à leur responsabilité en matière de protection de ces actifs.

Ils doivent :

- Consulter les services des technologies de l'information pour une analyse des risques de tous les projets informatiques ;
- Participer à la catégorisation des informations relevant de leur responsabilité en termes de sensibilité, de disponibilité, d'intégrité et de confidentialité ;
- Participer à toutes les activités de gestion des risques, y compris l'évaluation, la détermination du niveau de protection cible, l'élaboration de contrôles et la gestion des risques résiduels ;
- Veiller à la mise en œuvre et à l'application des mesures de sécurité de l'information, y compris celles liées au respect de la confidentialité au sein de leur service ;
- Veiller à la sécurité de toutes les ressources informationnelles qui leur sont confiées en leur qualité de garants. Exemples : gestion des identités et des accès (GIA), gestion des niveaux de risque, etc. ;

- Participer à des activités de formation et de sensibilisation à la cybersécurité et veiller à ce que les employés sous leur supervision y participent activement ;
- Signaler tout événement ou toute menace liée à la sécurité de l'information aux services informatiques ;
- Veiller à ce que les exigences en matière de sécurité de l'information soient prises en compte dans tous les processus d'approvisionnement et les contrats de service relevant de leur responsabilité, et à ce que tous les consultants externes, les fournisseurs, les partenaires, les invités, les organisations et les entreprises acceptent de se conformer à la politique et à tous les autres éléments du cadre de gestion de la sécurité de l'information ;
- Signaler toute violation ou tout problème lié à l'application de la Politique au CSIO.

6.11. Personnel du Collège

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs des ressources informationnelles du Collège. Le personnel qui y accède, la consulte ou la traite est responsable de son utilisation et doit agir pour la protéger.

À cette fin, le personnel du Collège doit :

- Se conformer à la politique et à toutes les autres directives et lignes directrices du Collège relatives à la sécurité de l'information et l'utilisation des actifs informationnels ;
- Être responsable des actions résultant de l'utilisation de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient effectuées par lui-même ou par un tiers, à moins qu'il ne puisse démontrer que ces actions ne résultent pas de sa négligence ou de sa mauvaise foi ;
- Se conformer aux exigences légales concernant l'utilisation de produits (licences, logiciels, progiciels, applications et services infonuagiques) ou de documents pouvant faire l'objet de droits de propriété intellectuelle ;
- Informer la direction de toute situation susceptible de compromettre la sécurité des actifs informationnels ;
- Participer à la catégorisation des informations du département selon les besoins ;
- Participer à des formations et à des activités de sensibilisation à la cybersécurité ;
- Utiliser les droits d'accès attribués et autorisés ainsi que les informations et les systèmes mis à leur disposition uniquement dans le contexte et aux fins pour lesquels ils sont destinés ;
- Respecter les mesures de sécurité en vigueur. Ne pas les contourner, les modifier ou les enfreindre ;
- Signaler immédiatement aux services des technologies de l'information tout incident lié à la sécurité de l'information dont ils ont connaissance (piratage ou intrusion dans un système informatique, usurpation d'identité, utilisation de virus informatiques, etc.) ;
- Participer à toute action entreprise pour identifier ou atténuer une menace ou un incident lié à la sécurité de l'information.

6.12. Étudiants

Les étudiants doivent :

- Se conformer à la politique et à toutes les autres directives et lignes directrices du Collège relatives à la sécurité de l'information et à l'utilisation des ressources informatiques ;
- Être responsables des actions résultant de l'utilisation de leur identifiant, de leur code d'accès ou de leur mot de passe, que ces actions soient effectuées par eux-mêmes ou par un tiers, à moins qu'ils ne puissent démontrer que ces actions ne résultent pas de leur négligence ou de leur mauvaise foi ;
- Se conformer aux exigences légales concernant l'utilisation de produits (licences, logiciels, progiciels, applications et services infonuagiques) ou de documents pouvant faire l'objet de droits de propriété intellectuelle ;
- Signaler à un membre du corps enseignant ou à un autre membre du personnel du Collège toute situation susceptible de compromettre la sécurité d'un actif informationnel ;
- Utiliser les droits d'accès attribués et autorisés ainsi que les informations et les systèmes mis à leur disposition uniquement dans le contexte et aux fins pour lesquels ils sont destinés ;
- Respecter les mesures de sécurité en vigueur. Ne pas les contourner, les modifier ou les enfreindre ;
- Signaler immédiatement à un membre du corps enseignant ou aux services des technologies de l'information tout incident lié à la sécurité de l'information dont ils ont connaissance (piratage ou intrusion dans un système informatique, usurpation d'identité, utilisation de virus informatiques, etc.) ;
- Participer à toute action entreprise pour identifier ou atténuer une menace ou un incident lié à la sécurité de l'information.

7. Principes directeurs

7.1. Responsabilité

- Chacun a un rôle à jouer dans la protection des informations et la garantie de leur sécurité.
- L'efficacité des mesures de sécurité de l'information dépend en partie de l'attribution de responsabilités et d'obligations de rendre compte aux utilisateurs.
- Le Collège fournit aux utilisateurs les divers appareils et logiciels nécessaires à l'exercice de leurs fonctions telles que déterminés par le Collège. Les utilisateurs assument une responsabilité spécifique quant à l'utilisation de cet équipement et de ces logiciels qui leur sont attribués et sont donc responsables de leurs actions. Le Collège prendra les mesures nécessaires pour s'assurer que l'équipement est utilisé correctement.

7.2. Droit d'inspection

Le Collège est propriétaire de ses actifs informationnels et peut donc déterminer comment ils sont utilisés par un utilisateur. Conformément aux lois et règlements en vigueur, le Collège est en droit d'inspecter toute utilisation de ses actifs informationnels.

7.3. Sécurité de l'information[1]

Le Collège adhère aux principes des meilleures pratiques en matière de sécurité de l'information, s'appuie sur les normes internationales pertinentes pour promouvoir leur utilisation et réalise des analyses comparatives avec des organisations ou des institutions similaires.

Le Collège adhère également à une approche acceptable fondée sur les risques, en établissant un cadre de gestion de la sécurité de l'information permettant d'ajuster les risques grâce à une combinaison de mesures raisonnables visant à assurer la sécurité de l'information.

La sécurité de l'information repose sur les trois principes suivants :

7.3.1. Disponibilité

La disponibilité garantit aux utilisateurs autorisés d'un système un accès rapide et ininterrompu aux informations qu'il contient ainsi qu'au réseau. Les informations doivent être accessibles à temps et sous la forme requise par l'utilisateur. Des mesures de contrôle doivent être mises en place pour garantir cette disponibilité.

7.3.2. Intégrité

L'intégrité des données garantit qu'elles n'ont subi aucune altération pendant leur communication, qu'elles soient au repos, en transit ou en mémoire. Des mesures de sécurité d'accès physiques et logiques doivent être mises en place pour garantir cette intégrité.

7.3.3. Confidentialité

La confidentialité vise à empêcher l'accès non autorisé à des informations sensibles. Son objectif est de garantir que seules les personnes autorisées y aient accès. La confidentialité des informations doit également être maintenue tout au long de leur cycle de vie. Des mesures de contrôle doivent être mises en place pour garantir cette confidentialité.

[1] Publication SP800-53 du NIST

7.4. Catégorisation des informations

Les informations sont une ressource cruciale qui doit être protégée tout au long de leur cycle de vie. C'est pourquoi il est essentiel de tenir à jour un inventaire de l'ensemble des ressources informationnelles du Collège. La première étape de la sécurité de l'information consiste à évaluer la sensibilité de ces ressources. La catégorisation de ces ressources en matière de sécurité de l'information est un processus qui permet d'évaluer leur degré de sensibilité afin de déterminer leur niveau de protection.

Il est important de réévaluer périodiquement la catégorisation des actifs informationnels afin de s'assurer qu'elle reste appropriée au regard des changements dans les obligations légales et contractuelles, ainsi que dans l'utilisation des données ou leur valeur pour le Collège. Cette évaluation doit être effectuée par le garant des actifs.

8. Cadre de gestion

La mise en œuvre de cette politique repose sur la mise en place d'un cadre de gestion de la sécurité de l'information du Collège, qui définit le champ d'action des différentes parties prenantes. Ce cadre de gestion précise les aspects fonctionnels de la sécurité de l'information, permet de définir des objectifs clairs et d'assurer une responsabilité appropriée.

Les pratiques et solutions de sécurité de l'information sont réévaluées périodiquement pour tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des risques et des menaces.

La politique de sécurité de l'information du Collège repose sur cinq principes de gestion fondamentaux :

8.1. Gestion des identités et des accès (GIA)

La gestion des identités et des accès est surveillée et contrôlée afin de garantir que l'accès, la divulgation et l'utilisation de toutes les informations détenues par le Collège sont strictement limités aux personnes autorisées, et ainsi protéger la confidentialité.

Les renseignements confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, comprennent les données personnelles ainsi que tout renseignement dont la divulgation porterait préjudice aux relations intergouvernementales, aux négociations entre organisations, à l'économie, aux tiers en ce qui concerne leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, à l'administration de la justice, à la sécurité publique, aux décisions administratives ou politiques, ainsi qu'aux vérifications.

8.2. Gestion des vulnérabilités

La gestion des vulnérabilités consiste à prendre des mesures pour maintenir à jour les logiciels et le matériel informatique, afin de minimiser les vulnérabilités et de réduire le risque de cyberattaque. Un système doit être mis en place pour gérer les rapports de vulnérabilité provenant des fournisseurs ou des prestataires de services, afin qu'ils puissent être évalués et, le cas échéant, corrigés.

8.3. Gestion des risques

La gestion des risques liés aux actifs informationnels du Collège repose sur une analyse des menaces pesant sur l'intégrité, la disponibilité et la confidentialité des informations détenues par l'établissement. Cette analyse est utilisée de manière récurrente pour établir des lignes directrices et des directives concernant l'utilisation et le fonctionnement des systèmes d'information, ainsi que les résultats attendus.

L'analyse des risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, qu'ils soient locaux ou distants, détenus ou externalisés, en précisant les mesures de sécurité à mettre en œuvre pour les utiliser dans l'environnement du collège.

Tous les risques susceptibles d'affecter les opérations ou la réputation du gouvernement sont signalés conformément à la directive gouvernementale sur la sécurité de l'information.

8.4. Gestion des incidents

La gestion des incidents consiste à mettre en œuvre des procédures pour signaler, analyser et répondre aux incidents de sécurité. Ces mesures visent à garantir la continuité du service. Elle permet également au Collège d'exercer son autorité et ses prérogatives en cas d'utilisation inappropriée des actifs informationnels.

Tous les incidents susceptibles d'affecter les opérations ou la réputation du gouvernement sont signalés conformément à la directive gouvernementale sur la sécurité de l'information. (CERT/QC)

8.5. Gestion de la continuité et de la reprise des activités

La gestion de la continuité et de la reprise des activités après sinistre consiste à mettre en œuvre des processus permettant d'identifier les incidents opérationnels majeurs susceptibles de menacer le Collège, tels que les catastrophes naturelles, les pannes d'électricité ou de télécommunications, les pannes informatiques, le piratage, le terrorisme, les pandémies, etc. Cette identification nous permet d'évaluer leur impact sur les activités du Collège et de prendre les mesures d'atténuation nécessaires pour assurer la continuité des activités essentielles.

9. Formation, sensibilisation et information

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

Les membres de la communauté du Collège doivent être sensibilisés aux points suivants :

- Les attentes du Collège en matière de sécurité de l'information et des systèmes d'information ;
- Les conséquences d'une violation de la sécurité ;
- Leurs rôles et responsabilités en matière de sécurité de l'information.

Le Collège s'engage à former et à sensibiliser régulièrement les utilisateurs à la sécurité des actifs informationnels. Il revient à l'utilisateur de participer à ces activités.

10. Révision de cette politique

La politique sera révisée si nécessaire, mais au moins tous les cinq ans à compter de sa date d'adoption.

11. Date d'entrée en vigueur

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

12. Sanctions

Toute personne qui enfreint la politique ou incite une autre personne à le faire est personnellement responsable, de même que toute personne qui, par négligence ou omission, entraîne une protection inadéquate des informations.

Tout employé ou étudiant du Collège qui enfreint le cadre juridique, la politique et les mesures de sécurité de l'information qui en découlent peut faire l'objet de sanctions, conformément aux lois applicables, aux règles administratives ou disciplinaires internes (y compris celles contenues dans les conventions collectives et les règlements du Collège), en fonction de la nature, de la gravité et des conséquences de l'infraction.

Toute violation de la politique, qu'elle soit commise par un fournisseur, un partenaire, un invité, un consultant ou un organisme tiers, sera passible des sanctions prévues dans le contrat qui les lie au Collège ou en vertu des lois et règlements applicables.