CHAMPLAIN
REGIONAL COLLEGE

Cadre de gestion de la sécurité de l'information

Champlain
COLLEGE LENNOXVILLE

1958
St.Lawrence
CEGEP CHAMPLAIN

Champlain
COLLEGE SAINT-LAMBERT

Historique des révisions

Version	Date	Par	Type	Commentaires
0.1	11 juillet 2024	Claude Leduc	Création	
0.2	20 août 2024	Claude Leduc	Modification	Ajoutée 6.2.4
1.0	19 septembre 2024	Claude Leduc	Approbation	Approuvé par le directeur général

Table des matières

1. Préambule

Le présent cadre vient compléter la politique de sécurité de l'information[1] . Il découle de la Directive gouvernementale sur la sécurité de l'information, laquelle exige des organismes publics qu'ils adoptent, mettent en œuvre, maintiennent et appliquent un tel cadre.

Il s'applique aux organismes publics visés par la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. Son objectif est de renforcer la gouvernance de la sécurité de l'information au sein du Collège régional Champlain, ci-après appelé « le Collège », en mettant en place une structure organisationnelle dédiée à la sécurité de l'information et en définissant les rôles et responsabilités à tous les niveaux de l'organisation. Il vise également à instaurer une vision commune de la sécurité de l'information et à garantir la cohérence et la coordination des actions dans ce domaine.

2. Cadre juridique et réglementaire

Ce cadre de gestion repose principalement sur :

- 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 (LRQ, c. C-1.1)
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, c. A-2.1)
- Règlement sur les incidents de confidentialité (LRQ, c. 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, c. 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)
- 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)
- 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

[1] https://www.crc-sher.qc.ca/college-champlain/governance-documentation/

- Exigences du *Ministère de la Cybersécurité et du Numérique (MCN)* et des *Centres opérationnels de cyberdéfense (COCD)*
- Tous les règlements, politiques et règlements du Collège
- Toute autre loi ou réglementation applicable.

3. Champ d'application

Ce cadre couvre les domaines d'application adoptés dans le cadre de la politique de sécurité de l'information.

Il aborde également tous les aspects de la gestion et de la protection des informations, notamment :

- Les informations sensibles ou confidentielles ;
- Les informations stratégiques ou critiques ;
- Les informations publiques ;
- Les réseaux internes, le nuage et les systèmes utilisés pour sauvegarder, traiter ou transmettre des informations ;
- Les bases de données et les applications utilisées pour gérer les informations ;
- Les appareils et périphériques (ordinateurs, ordinateurs portables, téléphones, imprimantes, scanners, etc.) utilisés pour y accéder ;
- Documents et supports de sauvegarde (papier, disques durs, clés USB, etc.) utilisés pour stocker des informations ;
- Communications électroniques (courriel, messagerie instantanée, etc.) utilisés pour transmettre ou recevoir des informations.

4. 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.

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*.

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.

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.

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.

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.

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.

5. Principes directeurs

Ce cadre de gestion de la sécurité de l'information vient compléter l'application de la politique de sécurité de l'information du Collège. Il précise les aspects fonctionnels de la sécurité de l'information.

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

Le cadre de gestion de la sécurité de l'information du Collège repose sur cinq principes directeurs :

5.1. 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.

5.2. 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.

5.3. 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 le Collège. Cette analyse est utilisée de manière récurrente pour établir des lignes directrices et des directives relatives à l'utilisation et au fonctionnement des systèmes d'information, ainsi qu'aux 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.

5.4. 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. (au CERT/QC)

5.5. 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.

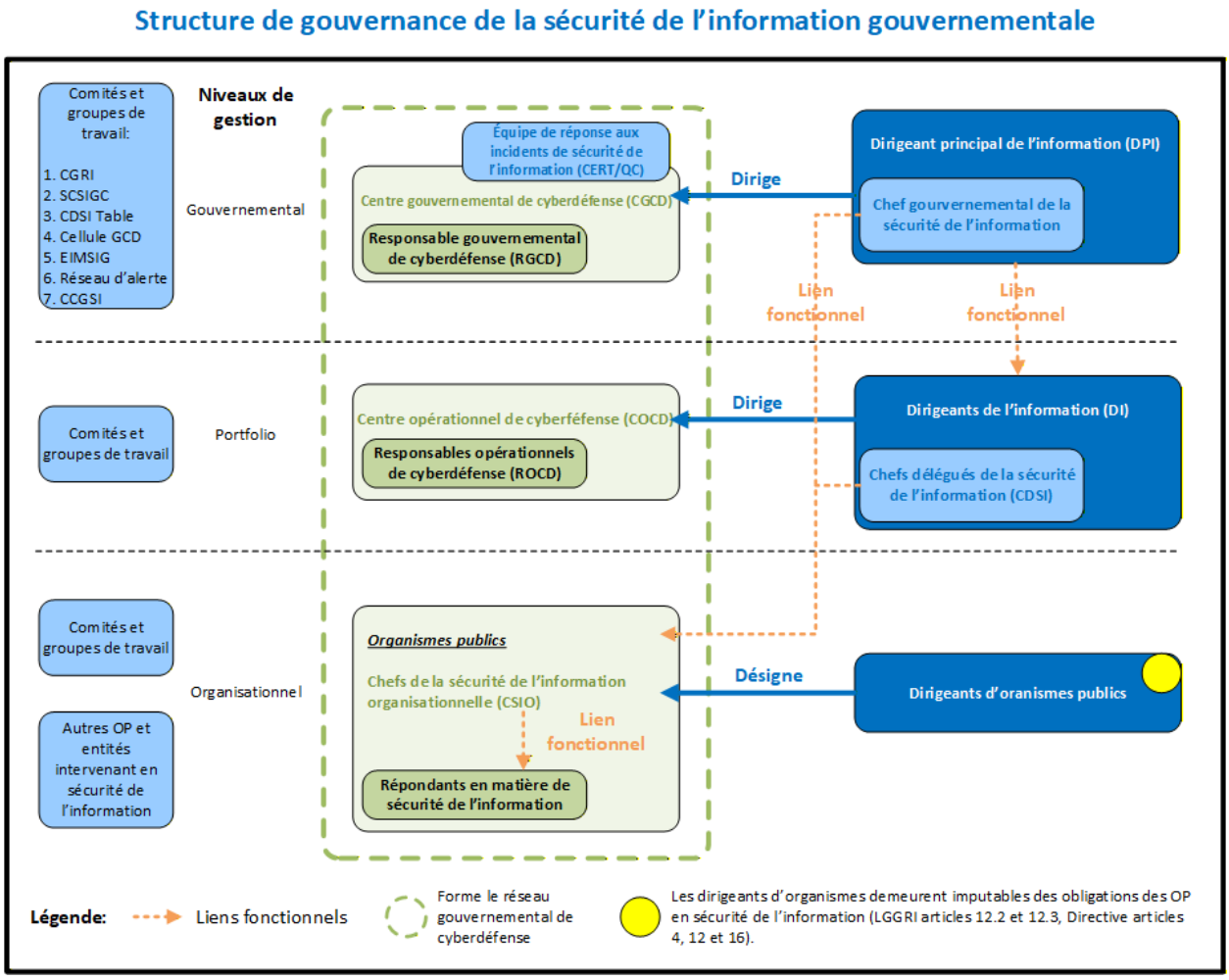
6. ORGANISATION FONCTIONNELLE DE LA SÉCURITÉ DE L'INFORMATION

La sécurité de l'information au sein du Collège requiert une structure organisationnelle conforme au cadre gouvernemental de gestion de la sécurité de l'information. Une telle structure doit permettre d'établir une gouvernance sectorielle forte et intégrée, favorisant une action concertée entre les parties prenantes et leur permettant de tirer parti de la complémentarité de leurs ressources et de l'efficacité de leurs actions.

6.1. Structure gouvernementale

L'organisation fonctionnelle de la sécurité de l'information au sein de l'administration publique, conformément à la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, ainsi qu'à la Directive gouvernementale sur la sécurité de l'information, repose sur une structure de gouvernance définie en trois niveaux de gestion :

- Niveau gouvernemental (ministère de la cybersécurité et du numérique (MCN)).
- Niveau du portefeuille (ministère de l'enseignement supérieur).
- Niveau organisationnel (le Collège).



Source figure 1 : Structure de gouvernance de la sécurité de l'information gouvernementale (*Cadre gouvernemental de gestion de la sécurité de l'information*, août 2022)

Les responsables de la sécurité de l'information pour des domaines spécifiques sont nommés par le directeur de leur organisme public respectif, à la demande du Chef de la sécurité de l'information du gouvernement (CGSI), conformément à l'article 11 de la directive gouvernementale sur la sécurité de l'information. Dans le cadre de l'organisation fonctionnelle de la sécurité de l'information, ces responsables assument les responsabilités indiquées par le CGSI.

6.2. Organisation fonctionnelle de la sécurité de l'information pour le Collège

6.2.1. Directeur général

Le directeur général est le premier responsable des informations dont il a la charge. Il est également chargé d'appliquer les lois définissant le cadre juridique de la gestion de l'information.

À ce titre, il veille au respect des lois et règlements établis par le Conseil du trésor, notamment en ce qui concerne la mise en œuvre de mesures visant à réduire les risques pesant sur les ressources informationnelles, et ce, en améliorant la sécurité de l'information. Il veille à ce que les différents éléments structurels de la sécurité de l'information soient mis en œuvre, tenus à jour et communiqués au Dirigeant de l'information (DI) du ministère de l'enseignement supérieur. Pour l'aider dans l'exercice de ses fonctions, il est préférable qu'il recrute du personnel qualifié aux niveaux stratégique, tactique et opérationnel, ou qu'il partage l'expertise existante avec d'autres institutions de son réseau.

Ces ressources seront respectivement désignées sous les noms de « chef de la sécurité de l'information organisationnelle » (CSIO) et de « coordonnateurs organisationnels des mesures de sécurité de l'information » (COMSI).

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

Le chef de la sécurité de l'information organisationnelle (CSIO) est chargé de la gestion globale de la sécurité de l'information au sein de l'organisation. Il travaille en étroite collaboration avec les promoteurs de la sécurité de l'information pour garantir le respect des exigences en la matière. Au sein de l'organisation fonctionnelle chargée de la sécurité de l'information, le CSIO a les responsabilités suivantes :

- Mettre en œuvre les décisions prises par le chef gouvernemental de la sécurité de l'information (CGSI) et le chef délégué de la sécurité de l'information (CDSI) ;
- Contribuer à la mise en œuvre du cadre de gouvernance de la sécurité de l'information au sein de l'organisation ;
- Contribuer à la mise en œuvre des processus normalisés de gestion de la sécurité de l'information du gouvernement et des processus de sécurité de l'information élaborés par le chef délégué de la sécurité de l'information (CDSI) ;
- Veiller à ce que les exigences en matière de sécurité de l'information soient prises en compte lors du développement, de l'acquisition, de l'évolution ou du remplacement d'un actif informationnel ou d'un service de ressources informationnelles ;
- Informer immédiatement le chef délégué de la sécurité de l'information (CDSI) lorsqu'un événement de sécurité présente un risque de préjudice grave ;
- Mettre en œuvre les mesures nécessaires pour faire face à un événement ou à un incident lié à la sécurité de l'information ;
- Tenir un registre des événements liés à la sécurité de l'information conformément aux exigences de la directive gouvernementale sur la sécurité de l'information et aux procédures spécifiées par le chef délégué de la sécurité de l'information (CDSI) ;
- Fournir au chef gouvernemental de la sécurité de l'information (CGSI) et au chef délégué de la sécurité de l'information (CDSI), auxquels ils rendent compte, les informations demandées à des fins de responsabilité ou à leur demande ;
- Assurer la coordination des activités de sécurité de l'information entreprises par toutes les parties prenantes au sein du Collège ;

- Mettre en place et coordonner des comités et des groupes de travail appropriés au sein de l'organisation pour traiter les questions de sécurité de l'information ;
- Veiller au développement des compétences des employés de l'organisation en matière de sécurité de l'information grâce à un plan continu de formation et de sensibilisation à la sécurité de l'information.

6.2.3. Coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI)

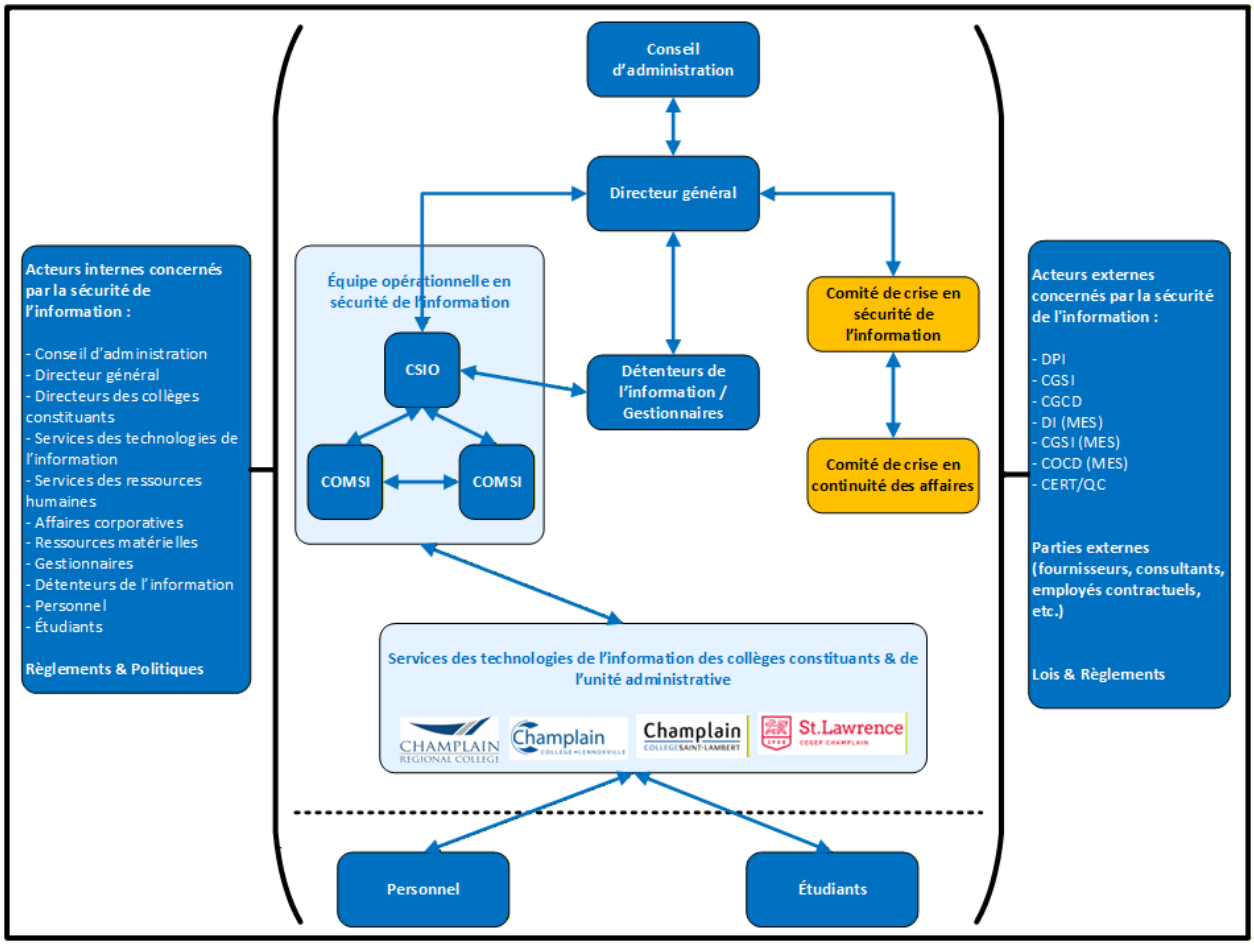
- Les COMSIs représentent le Collège au sein du réseau d'alerte gouvernemental. Ils sont chargés de mettre en œuvre le processus de gestion des menaces, vulnérabilités et incidents (GMVI) du Collège, ainsi que d'assister le chef de la sécurité de l'information organisationnelle (CSIO). Outre leurs responsabilités en matière de gestion des événements liés aux GMVI, les COMSIs représentent le Collège et participent activement au réseau d'alerte gouvernemental coordonné par le CERT/QC ;
- Identifier les GMVI affectant le Collège, en informer le CSIO et les escalader de manière appropriée selon les termes définis dans le processus GMVI ;
- Veiller à ce qu'un plan d'intervention interne en cas de GMVI soit élaboré, mis à jour et mis en œuvre ;
- Veiller à ce que des évaluations des risques de sécurité soient effectuées ;
- Travailler en étroite collaboration avec le CSIO et le ROCD afin de leur fournir le soutien technique nécessaire à l'exercice de leurs responsabilités.

6.2.4. Équipe opérationnelle chargée de la sécurité de l'information

- L'équipe opérationnelle chargée de la sécurité de l'information est une équipe interne dirigée par le chef de la sécurité de l'information organisationnelle (CSIO) et les deux coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI) ;
- L'objectif principal de cette équipe est de veiller à ce que la politique de sécurité de l'information et le cadre de gestion de la sécurité de l'information soient appliqués au sein de l'organisation ;
- Cette équipe est également responsable devant ses homologues gouvernementaux, conformément au point 6.1 ci-dessus. À ce titre, elle doit répondre aux demandes, requêtes, protocoles, instructions et directives de ces derniers ;
- Cette équipe doit également assister à des événements hebdomadaires consacrés à la sécurité de l'information. Il s'agit, par exemple, des réunions hebdomadaires du CERT/QC, de la réunion préparatoire sur les menaces du centre de cyberdéfense, etc. ;
- Cette équipe est le principal point de contact et de collaboration avec les équipes internes des collèges constituants ;
- Enfin, cette équipe est le principal groupe de coordination dans le processus de gestion des incidents.

6.3. Structure organisationnelle de la sécurité de l'information du collège

Structure organisationnelle de la sécurité de l'information de Collège Régional Champlain



7. Rôles et responsabilités

Pour que les mesures de sécurité de l'information soient efficaces, il est essentiel que les rôles et responsabilités de chaque partie prenante au sein du collège soient clairement définis.

7.1. 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, ainsi qu'à l'application de la politique de sécurité de l'information et du présent cadre de gestion de la sécurité de l'information.

Le directeur général approuve également le cadre de gestion de la sécurité de l'information.

7.2. Directeur du 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 déléguée par le directeur général. À ce titre, il veille au respect et à l'application des lois et règlements en la matière, à la mise en œuvre du cadre gouvernemental de sécurité de l'information, ainsi qu'à l'application de la politique de sécurité de l'information et du présent cadre de gestion de la sécurité de l'information au sein de son établissement.

7.3. Affaires corporatives

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

7.4. Services des technologies de l'information

Les services des technologies de l'information sont chargés de mettre en œuvre la politique de sécurité de l'information et le présent cadre de gestion de la sécurité de l'information au sein de 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 d'information, ainsi que lors de la mise en œuvre de projets de développement ou d'acquisition de systèmes d'information.

Les services des technologies de l'information aident le CSIO et les COMSIs à gérer, à mettre en œuvre et à rendre compte de toutes les questions liées à la sécurité de l'information, conformément aux lois, règlements et cadres gouvernementaux en vigueur.

7.5. Services des ressources humaines

En matière de sécurité de l'information, les services des ressources humaines doivent informer tous les nouveaux employés du Collège de la politique de sécurité de l'information et du présent cadre de gestion de la sécurité de l'information, et obtenir leur engagement à les respecter.

7.6. Services des ressources matérielles

Les services des ressources matérielles, y compris les services liés aux bâtiments et à l'équipement, collaboreront avec le CSIO pour déterminer les mesures de sécurité physique nécessaires à la protection des actifs informationnels du collège.

7.7. Les gestionnaires

Les gestionnaires sont les garants des actifs informationnels dont ils ont la charge. Ils veillent au respect des règles, des cadres et des politiques applicables afin de garantir l'accessibilité, l'utilisation appropriée et la sécurité des actifs informationnels dont ils ont la charge.

Les gestionnaires doivent également :

- Valider la cohérence de l'accès basé sur le profil de chaque utilisateur ;
- 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 vie privée au sein de leur service ;
- Garantir la sécurité de toutes les ressources informationnelles qui leur sont confiées en leur qualité de garants ;
- Signaler tout événement ou menace lié 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 contrats de service relevant de leur responsabilité, et à ce que tous les consultants externes, fournisseurs, partenaires, invités, organisations et entreprises s'engagent à se conformer à la politique de sécurité de l'information ainsi qu'à tous les autres éléments du présent cadre de gestion de la sécurité de l'information.

7.8. Personnel du Collège

La responsabilité de la sécurité des informations incombe à tous les utilisateurs des actifs informationnels du collège. Le personnel qui y accède, les consulte ou les traite est responsable de leur utilisation et doit agir pour les protéger.

À cette fin, le personnel du Collège doit :

- Se conformer à la politique de sécurité de l'information et à toutes les autres directives et lignes directrices du Collège relatives à la sécurité de l'information et à l'utilisation des actifs informationnels ;
- Signaler à la direction toute situation susceptible de compromettre la sécurité des actifs informationnels ;
- 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 place. Ne pas les contourner, les modifier ou les enfreindre ;
- Informer immédiatement les services informatiques de tout incident lié à la sécurité de l'information (piratage ou intrusion dans un système informatique, usurpation d'identité, utilisation de virus informatiques, etc.) dont ils ont connaissance ;
- Participer à toute action entreprise pour identifier ou atténuer une menace ou un incident lié à la sécurité de l'information.

7.9. Étudiants

Les étudiants doivent :

- Se conformer à la politique de sécurité de l'information et à toutes les autres directives et lignes directrices du Collège relatives à la sécurité de l'information et à l'utilisation des actifs informationnels ;
- Signaler toute situation susceptible de compromettre la sécurité d'une ressource informationnelle à un membre du corps enseignant ou à un autre membre du personnel du Collège ;
- 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 place. Ne pas les contourner, les modifier ou les enfreindre ;
- Informer immédiatement un membre du corps enseignant ou les services informatiques de tout incident lié à la sécurité de l'information (piratage ou intrusion dans un système informatique, usurpation d'identité, utilisation de virus informatiques, etc.) dont ils ont connaissance ;
- Participer à toute action entreprise pour identifier ou atténuer une menace ou un incident lié à la sécurité de l'information.

8. Diffusion et mise à jour du cadre de gestion

Le chef de la sécurité de l'information organisationnelle (CSIO), en collaboration avec le comité de direction (SMC), est responsable de la diffusion et de la mise à jour du présent cadre de gestion.

Ce cadre de gestion fera l'objet d'évaluations régulières, notamment en ce qui concerne la pertinence de ses déclarations par rapport aux nouveaux enjeux en matière de sécurité de l'information.

9. Date d'entrée en vigueur

Le présent cadre de gestion de la sécurité de l'information vient compléter la politique du Collège en la matière. Il entre en vigueur à la date de son approbation par le directeur général et reste en vigueur jusqu'à ce qu'il soit abrogé, modifié ou remplacé par un autre cadre de gestion.