Cégep de Sainte-Foy

CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

TABLE DES MATIERES

PRÉAMBULE

Le présent cadre vient en complément de la *Politique de sécurité de l'information*. Ce cadre de gestion découle de la *Directive sur la sécurité de l'information gouvernementale* qui oblige les organismes publics d'adopter et de mettre en œuvre un cadre de gestion de la sécurité de l'information, de le maintenir à jour et d'en assurer l'application.

Il s'applique aux organismes publics visés à l'article 2 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, ci-après appelée Loi. Il vise à renforcer la gouvernance de la sécurité de l'information du Cégep de Sainte-Foy, ci-après appelé le Cégep, par la mise en place d'une structure organisationnelle de la sécurité de l'information et la définition des rôles et responsabilités à tous les niveaux de l'organisation. Il vise également à établir une vision commune de la sécurité de l'information et à assurer la cohérence et la coordination des interventions en la matière. Il vient en complément de la *Politique de sécurité de l'information*.

Le cadre de gestion de la sécurité de l'information du Cégep aidera à implanter, graduellement, le cadre normatif du Cégep, disponible en annexe, tout en s'appuyant sur le cadre légal et le cadre normatif gouvernemental.

1. DÉFINITIONS

Continuité des services : Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

Plan de reprise informatique : Composante du plan de continuité des services, qui prévoit toutes les circonstances d'arrêt de l'exploitation des ressources informatiques, de même que les mesures curatives applicables à chacun des cas d'indisponibilité, afin que soit assurée, sur site ou hors site, la continuité des services.

Actif informationnel : Tout document dont la définition correspond à celle de l'article 3 et 4 de la *Loi concernant le cadre juridique des technologies de l'information* (chapitre C-1.1). Une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le Cégep habituellement accessible ou utilisable avec un dispositif des technologies de l'information (logiciel, progiciel, didacticiel, banque de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

Détenteurs de l'information : Gestionnaire participant à l'ensemble des activités relatives à la sécurité de l'information, notamment la gestion des risques, la détermination du niveau de protection (catégorisation de l'information) et la mise en place des actions correctives appropriées concernant les actifs informationnels.

Incident de sécurité : Événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

2. CADRE JURIDIQUE ET ADMINISTRATIF

Le cadre de gestion s'inscrit principalement dans un contexte régi par :

- La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*;
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1);
- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, r. 02);
- La *Directive sur la sécurité de l'information gouvernementale*; Guide d'élaboration d'un cadre de gestion de la sécurité de l'information;
- Le *Cadre gouvernemental de gestion de la sécurité de l'information*;
- Le *Cadre de gestion des risques et incidents à portée gouvernementale en matière de sécurité de l'information*;
- La *Politique de sécurité de l'information* du Cégep de Sainte-Foy.

3. CHAMP D'APPLICATION

Ce cadre traite les champs d'application approuvés dans la *Politique de sécurité de l'information*.

Concernant tous les aspects de la gestion et de la protection des informations, en regard aux :

- Données sensibles ou confidentielles;
- Données stratégiques ou critiques;
- Données publiques;
- Réseaux internes, infonuagiques et systèmes informatiques utilisés pour sauvegarder, traiter ou transmettre les informations;
- Bases de données et applications utilisées pour gérer les informations;
- Terminaux et périphériques (ordinateurs, téléphones, imprimantes, numériseurs, etc.) utilisés pour accéder aux informations;
- Documents et supports de sauvegarde (papier, disques durs, clés USB, etc.) utilisés pour enregistrer les informations;
- Communications électroniques (courriels, messagerie instantanée, etc.) utilisées pour transmettre ou recevoir les informations.

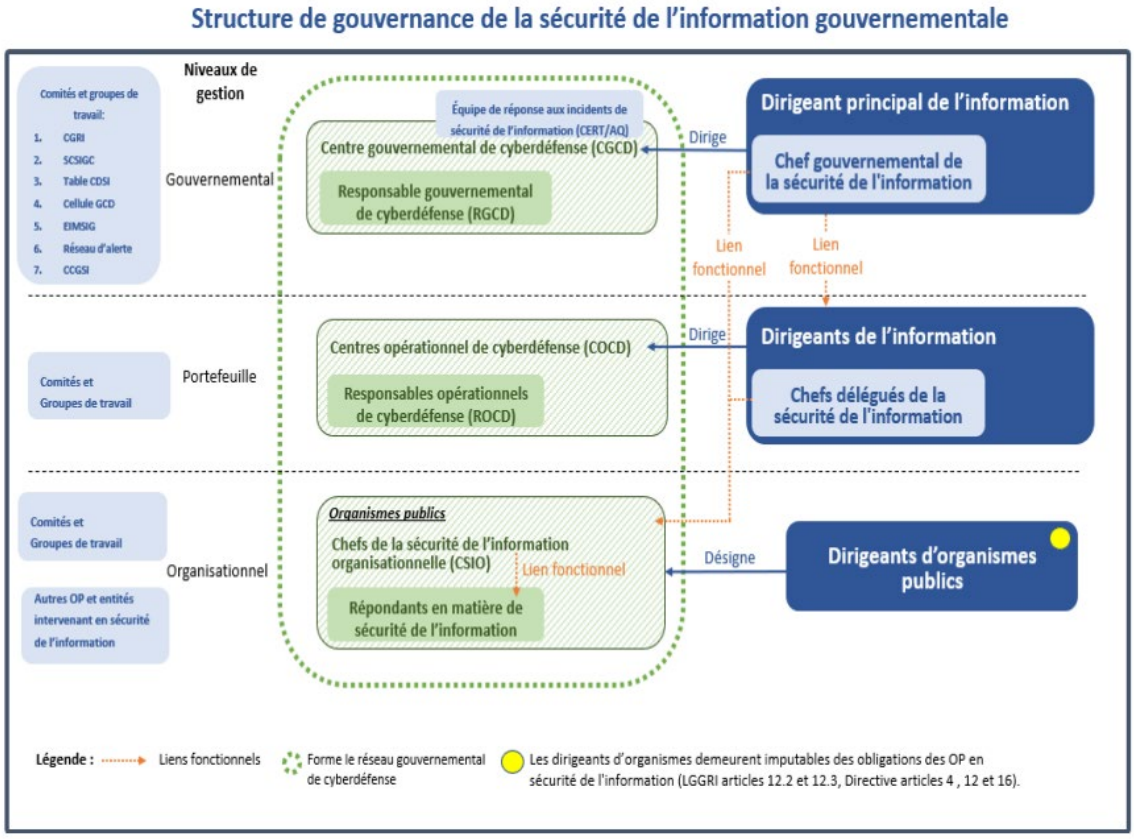
4. ORGANISATION FONCTIONNELLE DE LA SÉCURITÉ DE L'INFORMATION

La sécurité de l'information du Cégep passe par la mise en place d'une structure organisationnelle conforme au *Cadre gouvernemental de gestion de la sécurité de l'information*. Une telle structure doit répondre au besoin de mettre en place une gouvernance sectorielle, forte et intégrée, favorisant la concertation entre les intervenants et permettant de tirer avantage de la complémentarité de leurs ressources et de l'efficacité de leurs actions.

4.1 Structure gouvernementale

L'organisation fonctionnelle de la sécurité de l'information au sein de l'Administration publique s'articule, dans le respect de la Loi et la *Directive sur la sécurité de l'information gouvernementale*, autour d'une structure de gouvernance définie sur trois niveaux de gestion comme suit.

- Niveau gouvernemental (ministère de la Cybersécurité et du Numérique);
- Niveau portefeuille (ministère de l'Enseignement supérieur);
- Niveau organisationnel (Cégep de Sainte-Foy).



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

Les répondants en matière de sécurité de l'information, pour des domaines spécifiques en matière de sécurité de l'information, sont désignés par leur dirigeant d'organisme public respectif, à la demande du chef gouvernemental de la sécurité de l'information (CGSI) conformément à l'article 11 de la *Directive*. Ces répondants assument, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités qu'indique le chef gouvernemental de la sécurité de l'information (CGSI).

4.2 Organisation fonctionnelle de la sécurité de l'information pour le Cégep

Dirigeant d'organisme publics

Le dirigeant d'organisme est le premier responsable de l'information relevant de son autorité. Il est également le responsable de l'application des lois qui définissent le cadre juridique de la gestion de l'information.

À ce titre, il doit s'assurer du respect des lois et des règles déterminées par le Conseil du trésor, notamment en ce qui a trait à la mise en place de mesures permettant la réduction des risques des ressources informationnelles (RI) en améliorant la sécurité de l'information (SI). Il doit s'assurer que les divers éléments structurants de la sécurité de l'information soient mis en place, gardés à jour et communiqués au dirigeant de l'information (DI) du MES. Pour le soutenir dans l'exercice de ses fonctions, il est préférable qu'il se dote d'un personnel qualifié sur les plans stratégique, tactique et opérationnel ou qu'il partage, avec d'autres établissements de son réseau, des expertises déjà en place.

Ces ressources porteront le nom de « Chef de la sécurité de l'information organisationnelle » (CSIO) et respectivement « Coordonnateurs organisationnels des mesures de sécurité de l'information » (COMSI).

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

Un chef de la sécurité de l'information organisationnelle (CSIO) assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de son organisation. Il travaille en étroite collaboration avec les répondants en matière de sécurité de l'information pour assurer la prise en charge des exigences de sécurité de l'information. Il assume, dans l'organisation fonctionnelle de la sécurité de l'information, les responsabilités suivantes :

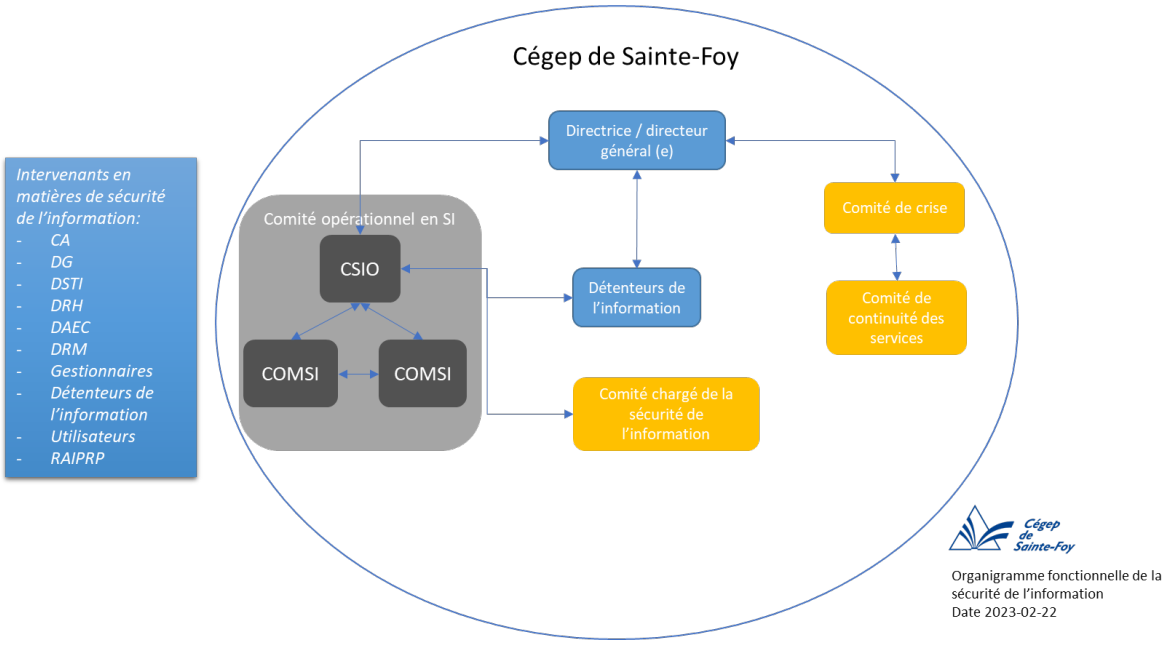
- Mettre en œuvre les décisions émanant du chef gouvernemental de la sécurité de l'information (CGSI) et du chef délégué de la sécurité de l'information (CDSI).
- Contribuer à la mise en œuvre du cadre de gouvernance qui régit la sécurité de l'information au sein de son organisation.
- Contribuer à la mise en œuvre des processus gouvernementaux normalisés en matière de gestion de la sécurité de l'information et des processus de sécurité de l'information élaborés par le chef délégué de la sécurité de l'information (CDSI).
- S'assurer de la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement, d'acquisition, d'évolution ou de remplacement d'un actif informationnel ou d'un service en ressources informationnelles.
- Aviser sans délai le chef délégué de la sécurité de l'information (CDSI) lorsqu'un événement de sécurité présente un risque qu'un préjudice sérieux soit causé.

- Mettre en œuvre les actions requises pour la prise en charge d'un événement ou incident de sécurité.
- Tenir un registre des événements de sécurité selon les exigences de la *Directive* et les modalités précisées par le chef délégué de la sécurité de l'information (CDSI).
- Fournir les informations demandées par le chef gouvernemental de la sécurité de l'information (CGSI) et le chef délégué de la sécurité de l'information (CDSI) auquel il se rattache relativement à la reddition de comptes, ou toute autre information requise par ces derniers.
- Assure la coordination des actions de sécurité de l'information menées au sein du Cégep par tous les intervenants.
- Mettre en place au sein de son organisation les comités et les groupes de travail appropriés de concertation en matière de sécurité de l'information et en assurer la coordination.
- Assurer le développement des compétences du personnel de son organisation en matière de sécurité de l'information à l'aide d'un plan en continu de formation et de sensibilisation en matière de sécurité de l'information.

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

- Le COMSI représente le Cégep auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (MVI) au Cégep, en plus de soutenir le chef de la sécurité de l'information organisationnelle (CSIO). En plus des responsabilités de la prise en charge d'événements associés à des MVI, le COMSI doit :Représenter le Cégep et participer activement au Réseau d'alerte gouvernemental, coordonné par le CERT/QC.
- Identifier les MVI touchant le Cégep, en tenir informé son CSIO et les faire remonter selon les conditions définies par le processus GMVI, si nécessaire.
- S'assurer de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux MVI.
- S'assurer de la réalisation d'analyses de risques de sécurité.
- Collaborer étroitement avec son CSIO et son responsable opérationnel de cyberdéfense (ROCD) en leur fournissant, notamment, le soutien technique nécessaire à l'exercice de leurs responsabilités.

4.3 Structure organisationnelle du Cégep



5. RÔLE ET RESPONSABILITÉ

Conseil d'administration

Le conseil d'administration approuve et adopte la *Politique sur la sécurité de l'information* du Cégep et ses orientations ainsi que toute modification subséquente à cette politique. De plus, il approuve le bilan de sécurité.

Direction générale

Agit à titre de première responsable de la sécurité de l'information. À ce titre, elle veille au respect et à l'application des lois et des règles de sécurité de l'information, à l'application du *Cadre gouvernemental de sécurité de l'information*, à l'application de la *Politique de sécurité de l'information* et du *Cadre de gestion de sécurité de l'information* au Cégep Sainte-Foy. Aussi, elle désigne les responsables organisationnels en sécurité de l'information.

Finalement, la Direction générale dépose le bilan de sécurité annuel au conseil d'administration concernant l'application de la *Politique de sécurité de l'information* et a le pouvoir d'appliquer les sanctions prévues dans cette dernière.

Direction des systèmes et des technologies de l'information (DSTI)

- Assurer la sécurité des services informatiques du Cégep. Il s'agit minimalement de la sécurité des informations et des données, des comptes et des identités, des appareils mobiles et des ordinateurs.
- Élaborer et s'assurer du respect d'un code d'éthique pour tous les membres du personnel de la DSTI.
- Participer activement à l'analyse de risques technologiques, à l'identification, à l'évaluation des besoins et des mesures à mettre en œuvre ainsi qu'à l'anticipation de toute menace en matière de sécurité faisant appel aux technologies de l'information.
- Appliquer des mesures de réaction appropriées à toute menace et à tout incident de sécurité de l'information lorsque les circonstances l'exigent, et ce, en vue d'assurer la sécurité de l'information en cause.
- Participer à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique.
- Élaborer et tenir à jour les documents portant sur la sécurité opérationnelle des actifs informationnels.
- S'assurer de la mise au rebut sécuritaire des supports de l'information.

Direction des ressources humaines

- Informer sans délai, l'ensemble des directions concernées d'une embauche, d'un changement de fonction et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels du Cégep.
- Informer tout nouvel employé de ses obligations découlant de la présente politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information et obtient son engagement à son respect.
- Vérifier les antécédents judiciaires des candidates et des candidats à certaines fonctions ciblées.
- Intervenir auprès des membres du personnel concerné en cas d'atteinte à la sécurité des technologies de l'information, en collaboration avec la DSTI et les autres intervenantes et intervenants.
- Contribuer à la promotion des activités de sensibilisation et des séances de formation pour les membres du personnel à la sécurité des actifs informationnels.

Direction des affaires étudiantes et des communications

- Est responsable de l'élaboration d'un plan de communication lié à la présente politique et du *Cadre de gestion de la sécurité de l'information*.
- Informe et sensibilise les membres de la communauté du Cégep (personnel et étudiante) sur leurs responsabilités en ce qui a trait à la sécurité de l'information en collaboration avec la DSTI.
- Informe la population étudiante de l'importance de l'application de la *Politique de la sécurité de l'information* et s'assure que tous les étudiants et toutes les étudiantes ont signé un engagement à cet effet.
- Élabore un plan de communication lors d'incidents en sécurité de l'information ayant un impact sur l'offre de services du Cégep en collaboration avec le comité de la sécurité de l'information (CSI).

Direction des ressources matérielles

- Gérer les moyens d'accès physique aux locaux à accès restreint.
- Concevoir et mettre en œuvre les mesures de protection physique contre les sinistres, les pertes, les dommages, le vol ainsi que l'interruption des activités, afin de sécuriser les lieux et les accès.
- Participer, avec la DSTI, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.
- Contrôler les accès physiques aux locaux du Cégep.
- Mettre à jour les informations dans la base de données des clés en suivant le mouvement du personnel au sein du Cégep.

Gestionnaires

- Informer et mettre en œuvre les dispositions de la *Politique de sécurité de l'information* auprès du personnel relevant de son autorité.
- Communiquer au CSIO tout élément important touchant la sécurité de l'information.
- S'assurer que la sécurité de l'information est prise en compte dans tout contrat de service attribué par son unité administrative et voir à ce que tout collaborateur, lié par contrat, respecte les règles de sécurité de l'information du Cégep.
- Accorder les accès à chacun des utilisateurs selon leur profil et tenir un registre.
- Vérifier la cohérence des accès selon les profils pour chacun des utilisateurs.

Détenteurs de l'information

- Catégoriser l'information relevant de leur responsabilité en matière de disponibilité, d'intégrité et de confidentialité.
- S'impliquer dans l'ensemble des activités relatives à la gestion des risques, notamment l'évaluation, la détermination du niveau de protection visé, l'élaboration des contrôles et la prise en charge des risques résiduels.
- Participer, lorsque requis, à la validation des orientations stratégiques, des politiques, des directives, des cadres de gestion, des guides, des plans d'action et des bilans.
- Veiller à la mise en place et à l'application des mesures de sécurité de l'information, y compris celles liées au respect des exigences de protection des renseignements personnels.
- S'assurer de la sécurité d'un ou plusieurs actifs informationnels qui leur sont confiés en tant que détenteur. Exemples : la gestion de l'identité et des accès, la gestion des niveaux de risque, etc.

Utilisateurs

- Prendre connaissance de la *Politique de sécurité de l'information* et s'engager par écrit à respecter cette dernière.
- Utiliser les technologies de l'information mises à sa disposition aux fins auxquelles elles sont destinées ainsi que dans le cadre des accès qui lui sont accordés.
- Se responsabiliser concernant l'utilisation de son identifiant, de son code d'accès ou de son mot de passe.
- Informer son responsable, son professeur ou la DSTI de toute violation des mesures de sécurité de l'information dont il pourrait être témoin.

Le comité de la sécurité de l'information et de protection des renseignements personnels

Il agit à titre de conseiller principal auprès du CSIO pour l'implantation de la stratégie reliée à la sécurité et la protection des données. Il évalue les risques et prodigue des recommandations pour les nouveaux projets et les activités d'exploitation associées aux actifs informationnels. De plus, il propose des actions concrètes afin d'implanter efficacement la politique, le cadre de gestion et le cadre normatif de sécurité.

Responsable de l'accès à l'information et de la protection des renseignements personnels (RAIPRP)

- Voir le *Cadre de gouvernance à l'égard de la protection des renseignements personnels*.

6. VALIDATION, APPROBATION ET COMMUNICATION

La validation du cadre de gestion nécessite la contribution de plusieurs intervenants compétents en la matière. Une fois approuvé, le cadre de gestion est diffusé, auprès de l'ensemble du personnel de l'organisation, en utilisant les moyens appropriés.

Il convient également d'organiser, à l'intention de l'ensemble du personnel, des séances de formation et de sensibilisation, afin de s'assurer d'une bonne compréhension des énoncés du cadre de gestion et de leur application par ce dernier.

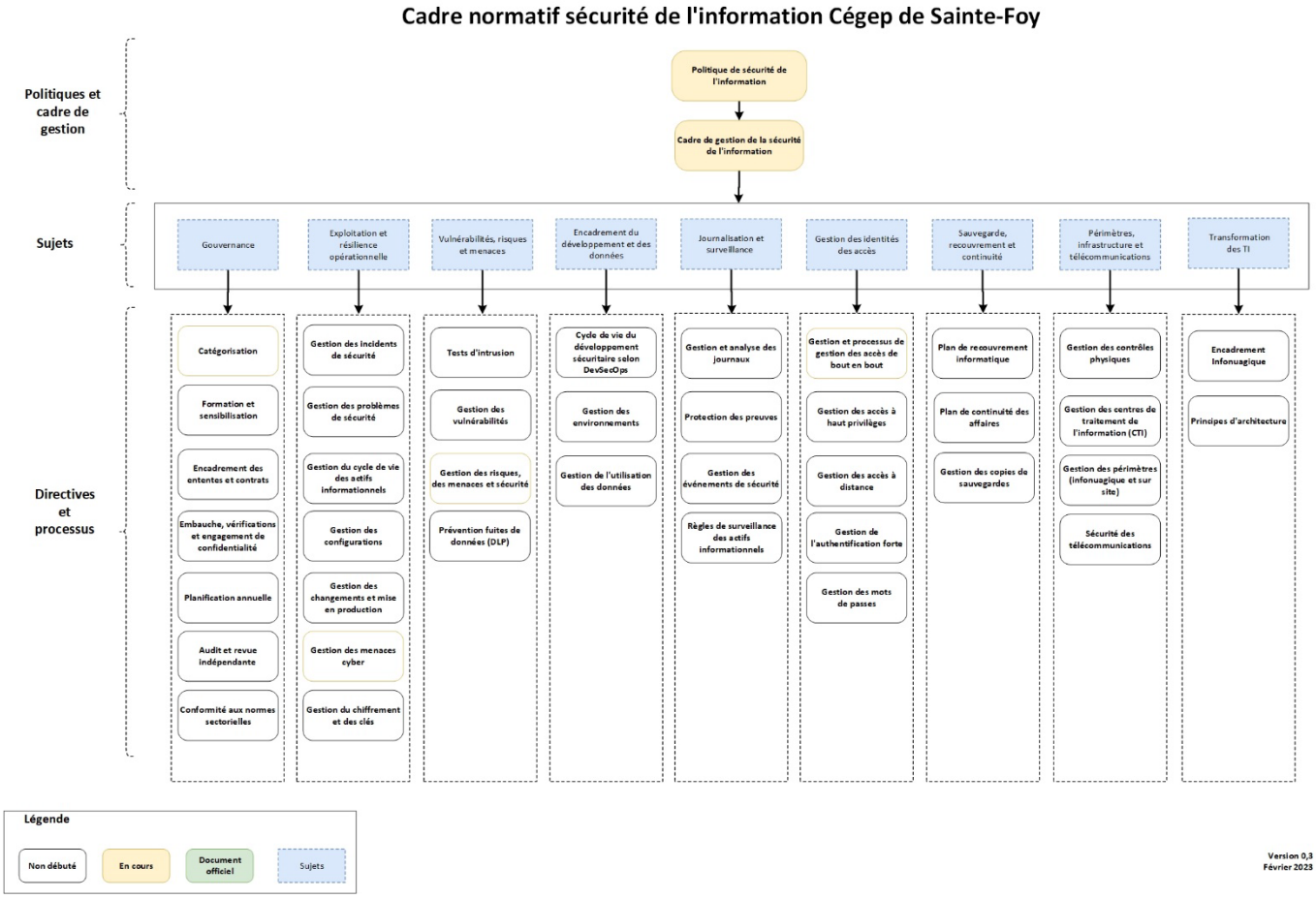
7. ENTRÉE EN VIGUEUR ET RÉVISION

Le présent *Cadre de gestion de la sécurité de l'information* est complémentaire à la *Politique sur la sécurité de l'information du Cégep*. Il entre en vigueur à la date de son approbation et suivant l'adoption de la *Politique* par le conseil d'administration. et demeure en application tant et aussi longtemps qu'il n'est pas abrogé, modifié ou remplacé par un autre cadre de gestion.

Le cadre de gestion est régulièrement évalué, notamment en ce qui a trait à la pertinence de ses énoncés à l'égard des nouveaux enjeux de sécurité de l'information. Une fois l'étape d'évaluation terminée, le cadre de gestion pourra faire l'objet d'une révision qui assurera l'adéquation de ses énoncés aux besoins de l'organisation en matière de sécurité de l'information.

Annexe 1 – Cadre normatif de la sécurité de l'information

Le *Cadre normatif de la sécurité de l'information* du Cégep est composé des règlements, processus, directives et avis qui traitent des aspects reliés à la sécurité des actifs informationnels du Cégep.



Ce cadre traitera sans s'y limiter des sujets suivants :

Gouvernance et formation
Ensemble des pratiques mises en place pour assurer la sécurité des systèmes d'information au sein d'une organisation. De plus, cette section comprend la formation et la sensibilisation des employés à ces pratiques.

Exploitation et résilience opérationnelle
Somme des pratiques, politiques et processus visant à maintenir de manière stable et sécuriser les actifs informationnels de l'organisation y compris lors des périodes de perturbation.

Vulnérabilités, risques et menaces
Manière dont les actifs informationnels sont gérés au quotidien au regard des fuites d'information, de la gestion des vulnérabilités, de l'évaluation des risques et des menaces, et ce, en continu. Pour y arriver, une série de processus, politique et directives doivent être développés.

Encadrement du développement et des données
Ensemble des pratiques, politiques, directives et procédures destinées à assurer la sécurité des données et des actifs informationnels tout au long de leur cycle de vie. Cette section comprend le développement d'une application ou d'un logiciel.

Journalisation, surveillance et audit
Pratiques visant à enregistrer et à encadrer les activités des utilisateurs et des actifs informationnels afin d'identifier de potentielles menaces tout en permettant d'obtenir des preuves et de les évaluer de manière objective.

Gestion des identités et des accès
Somme des politiques, procédures, règles et technologies permettant de gérer et d'encadrer les profils d'accès aux actifs informationnels et aux données de l'organisation.

Sauvegarde, recouvrement et continuité
Ensemble des pratiques et des politiques visant à protéger les données et les actifs informationnels de l'organisation en cas d'incident ou sinistre majeur. Ceci comprend le redémarrage le plus rapidement possible avec un minimum de perte de données.

Périmètres, infrastructures et télécommunications
Pratiques concernant les technologies, les politiques et les directives utilisées pour protéger les réseaux, les périmètres et les infrastructures physiques de l'organisation. L'adoption de l'infonuagique élargit les périmètres et complexifie le travail de protection des infrastructures.

Transformation des TI
Évolution des pratiques, des politiques et des technologies afin de répondre aux besoins grandissants de nos secteurs d'affaires.