CÉGEP DE VALLEYFIELD

Direction des affaires corporatives, du développement institutionnel et des communications

RECUEIL DE GESTION

TITRE: ***Politique de sécurité de l'information***

NUMÉRO : ***DTI-23-PO-02***

Responsable de l'application

- [ ] *Président du conseil d'administration*
- [ ] *Direction générale*
- [ ] *Direction de la formation continue*
- [ ] *Direction des études*
  - [ ] *Service du développement pédagogique et de l'encadrement scolaire*
  - [ ] *Service de l'organisation scolaire*
- [ ] *Direction des ressources humaines*
- [ ] *Direction des services administratifs*
  - [ ] *Service des finances*
  - [ ] *Service des ressources matérielles et des services communautaires*
  - [ ] *Service de l'approvisionnement*
- [X] *Direction des technologies de l'information*
- [ ] *Direction des affaires étudiantes*
- [ ] *Direction des affaires corporatives, du développement institutionnel et des communications*

Destinataires

- *Toute personne physique ou morale faisant usage des ressources informationnelles du Cégep.*

Approuvé par

- *Conseil d'administration*

Document de référence

Mise en application

- *Adoption : 24 octobre 2023*
- *Entrée en vigueur : 24 octobre 2023*
- *Révision :*
- *Modification :*

INTRODUCTION

Le Cégep de Valleyfield 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. Étant donné la valeur administrative, légale et financière de ses actifs informationnels, ils doivent faire l'objet d'une évaluation continue, d'une utilisation et d'une protection appropriées et adéquates tout au long de leur cycle de vie, selon les bonnes pratiques en la matière de sécurité informationnelle et avec une approche de gestion des risques, quel qu'en soit le support ou l'emplacement.

Les lois suivantes imposent des obligations importantes aux établissements collégiaux : 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 modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, 2021, chapitre 25), et la Directive gouvernementale sur la sécurité de l'information (2021) du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics.

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

ARTICLE 1 – OBJECTIFS DE LA POLITIQUE

La présente politique constitue le cadre général qui vise la gestion des actifs informationnels dans le respect des droits et obligations du Cégep 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 au 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 par l'entité autorisée ;
- Assurer l'intégrité de l'information en la préservant contre toute destruction, modification et altération de quelque façon sans autorisation et s'assurer que le support de cette information lui procure la stabilité et la pérennité voulues ;
- Préserver la confidentialité de l'information en s'assurant de ne pas la rendre accessible ou divulguée à des personnes, entités ou processus non autorisés ;
- Regrouper les lignes directrices et les rôles et responsabilités des intervenants en sécurité ;
- Identifier et classifier les actifs informationnels du Cégep selon leurs degrés de criticités et veiller constamment à leur évaluation ainsi que leur protection adéquate ;
- Assurer la conformité aux lois et cadres réglementaires ;
- Mettre en place un plan de continuité des activités et de relève informatique ;
- Assurer le respect de la vie privée des individus, notamment la confidentialité des renseignements personnels.

Par conséquent, le Cégep met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée et soutenue par le cadre de gestion de la sécurité de l'information de l'institution.

ARTICLE 2 – CADRE LÉGAL ET NORMATIF

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales.

- Le Code civil du Québec (LQ, 1991, chapitre 64) ;
- La Charte des droits et libertés de la personne (LRQ, chapitre C-12) ;
- Le Code criminel (LRC, 1985, chapitre C-46) ;
- La *Loi sur les archives* (LRQ, chapitre A-21.1) ;
- 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) ;
- La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25) ;
- La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C1.1) ;
- La *Loi sur l'Instruction publique* (LRQ, chapitre I-13.3) ;
- La *Loi sur la fonction publique* (RLRQ, chapitre F-3.1.1) ;
- La *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42) ;
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics ;
- La Directive gouvernementale sur la sécurité de l'information ;
- Le Cadre gouvernemental de gestion de la sécurité de l'information ;
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2) ;
- Le Règlement sur les incidents de confidentialité ;
- Le 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 ;*
- Les Dispositions légales et administratives en sécurité de l'information ;
- Les Règles relatives à la gestion des projets en ressources informationnelles ;
- Les Règles relatives à la planification et à la gestion des ressources informationnelles ;
- L'Aide-mémoire : Politique gouvernementale en cybersécurité ;
- Les conventions collectives et les contrats de travail ;
- Toute autre loi ou règle applicable.

Fondements normatifs

- 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.

ARTICLE 3 – CHAMP D'APPLICATION DE LA POLITIQUE

Personnes visées

Cette politique vise sans exception l'ensemble des personnes physiques et morales, régulières ou occasionnelles, peu importe son statut, appelées à utiliser les actifs informationnels du Cégep citant entre autres :

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

Actifs visés

La politique vise aussi toutes les informations et les actifs informationnels :

- Appartenant au Cégep
- Détenus par un tiers, mais appartenant au Cégep
- Utilisés et détenus par un tiers au bénéfice ou au nom du Cégep
- Et ce, quel que soit le support de conservation (électronique, technologique, papier, etc.).

Activités visées

Cette politique concerne l'ensemble des activités entrant dans le 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 Cégep que ce soient conduites dans le périmètre de ses locaux, dans un autre endroit ou à distance.

ARTICLE 4 - DÉFINITIONS

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 Cégep pour mener à bien sa mission.

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.

Cadre de gestion : l'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.

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 Cégep.

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.

Cycle de vie de l'information : l'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 Cégep.

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 manière adéquate par une personne autorisée.

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.

Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiées, ni altérées, ni détruites sans autorisation.

Membre du personnel : toute personne salariée, syndiquée ou non, incluant les cadres et les hors cadres, les travailleurs et travailleuses autonomes ainsi que les sociétés en nom collectif sous contrat avec le Cégep**.**

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 un sinistre majeur.

Réseau : Ensemble des composantes et des équipements informatiques reliés par voie de télécommunication en vue d'accéder à des actifs informationnels, ou de partager cet accès.

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

Direction des technologies de l'information (DTI) : équipe du Cégep incluant le directeur du service, mandatée pour gérer les flux de données, pour installer des équipements et des logiciels, pour entretenir et développer des réseaux informatiques et pour protéger les actifs informationnels et les données conservées sur les serveurs du Cégep ou ailleurs.

Technologies de l'information et des communications (TIC) : regroupent les techniques, principalement de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications (réseau filaire, sans fil et en collaboration avec 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.

ARTICLE 5 : RÔLES ET RESPONSABILITÉS

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

Direction générale

La Direction générale :

- Veille à l'application de la Politique sur la sécurité de l'information ;
- Approuve les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité et les redditions de comptes en matière de sécurité de l'information ;
- Veille à ce que le conseil d'administration soit informé, au moment opportun, des travaux en matière de sécurité de l'information ;
- Assume le processus de délégation des rôles de CSIO et COMSI ;
- Encadre le chef de la sécurité de l'information organisationnelle (CSIO) dans la réalisation de son mandat ;

Responsable de la protection des renseignements personnels

Le responsable de la protection des renseignements personnels veille à assurer le respect et la mise en œuvre de la loi sur la protection des renseignements personnels afin de mettre en œuvre des politiques et des pratiques encadrant la gouvernance des renseignements personnels.

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

La personne assumant la fonction de CSIO est un membre du personnel d'encadrement d'un organisme public. La fonction de CSIO est déléguée par la direction générale. Le CSIO est responsable de :

- La prise en charge globale de la sécurité de l'information au sein de son organisation ;
- La diffusion et de la mise en application de la politique ;
- 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) auquel il se rattache, notamment les indications d'application et les indications d'application particulières, en coordonner l'exécution et veiller à leur application ;
- 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 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 ;
- 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 ;

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

La personne assumant la fonction de COMSI agit sur le plan opérationnel. Elle intervient dans la mise en œuvre des mesures et apporte le soutien nécessaire au CSIO de l'établissement, notamment en matière de la gestion des incidents et des risques en sécurité de l'information.

Le COMSI représente l'organisme public auprès du Réseau d'alerte gouvernemental. Il est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) dans son cégep, en soutien à son chef de la sécurité de l'information organisationnelle (CSIO).

Il collabore auprès du CSIO du Cégep à l'élaboration des divers éléments stratégiques et tactiques en sécurité informationnelle :

- Maintiens le registre des événements et des incidents liés à la sécurité de l'information ;
- Effectue et participe aux analyses de risques en sécurité de l'information ;
- Gère le processus de gestion, de déclaration des incidents et de résolution de problème et contribue à sa mise en place ;
- Contribue au processus formel de gestion des droits d'accès à l'information.
- Représente le cégep et participe activement au Réseau d'alerte gouvernemental, coordonné par le CERT/QC (Équipe de réponse aux incidents de sécurité informationnelle du Gouvernement du Québec) ;
- Identifie les MVI touchant son cégep, en tient informé son CSIO et les fait remonter selon les conditions définies par le processus GMVI (Gestion des menaces, vulnérabilités et incidents), si nécessaire ;
- S'assure de l'élaboration, de la mise à jour et de l'application d'un plan interne de réponse aux MVI ;
- S'assure de la réalisation d'analyses de risques de sécurité ;
- Collabore 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.
- Effectue la veille technologique

Direction des technologies de l'information

La direction des technologies de l'information assume la responsabilité de l'application de la présente politique. Elle s'assure de la prise en charge des exigences de SI dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information.

De plus, elle participe, avec le CSIO, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep, 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.

Elle participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information.

Elle prend les mesures appropriées pour réagir aux menaces et aux incidents de sécurité de l'information, mesures pouvant aller jusqu'à l'interruption ou la révocation temporaire - lorsque les circonstances l'exigent - des services d'un système d'information faisant appel aux technologies de l'information.

Elle s'assure que les responsabilités des intervenants concernant la sécurité de l'information et le respect de la présente politique, ainsi que du cadre normatif des ressources informationnelles, sont inscrites dans les descriptions de tâches des membres de son personnel ;

Service des ressources matérielles

Le service des ressources matérielles participe, avec le responsable de la sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

Direction des ressources humaines

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

- Vérifier, au besoin, les antécédents des candidats à l'embauche et des membres du personnel impliqués dans la sécurité de l'information ;
- Informer et obtenir de tout nouvel employé du Cégep 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.

Direction des affaires corporatives, du développement institutionnel et des communications

À titre de responsable de la gestion documentaire et des archives, la DACDIC :

- Collabore à la conception des systèmes informatiques et administratifs dédiés à la gestion documentaire et s'assure qu'à toutes les étapes du cycle de vie de l'information, ces systèmes ont les qualités nécessaires pour permettre une saine gestion du patrimoine informationnel du Cégep et le respect des lois en vigueur en matière de conservation et d'archivage ;
- Collabore étroitement avec les responsables d'actifs informationnels ainsi qu'avec le CSIO en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support ;
- Est responsable de la protection des renseignements personnels ;
- Collabore à la communication et à la sensibilisation entourant la SI.

Responsable d'actifs informationnels (détenteur)

La personne assumant le rôle de responsable d'actifs informationnels est la personne-cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il ou elle :

- Participe à la catégorisation de l'information de l'unité sous sa responsabilité et à l'analyse de risques ;
- Veille à la protection de l'information et des systèmes d'information en conformité avec la politique de la SI ;
- Rapporte tout événement ou toute menace liée à la SI ;
- Collabore à la mise en œuvre de toute mesure pour améliorer la SI afin de remédier à un incident au besoin ;

Utilisatrices et utilisateurs

La responsabilité de la sécurité de l'information du Cégep incombe à toutes les utilisatrices et à tous les utilisateurs des actifs informationnels du Cégep. Tout utilisatrice ou utilisateur qui accède à une information, qui la consulte ou qui la traite, est responsable de l'utilisation qu'il ou elle en fait et doit procéder de manière à protéger cette information. À cette fin, l'utilisatrice ou l'utilisateur doit :

- Se conformer à la présente politique et à toute autre directive du Cégep 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 une personne responsable, un enseignant ou son supérieur immédiat, 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.
- Acheminer à la DTI toute demande relative à la mise en place ou à l'installation des actifs informationnels. Ces actifs doivent être préalablement autorisés.

ARTICLE 6 : ÉNONCÉ DES PRINCIPES GÉNÉRAUX

Protection de l'information[1]

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

- 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.

- 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.

- 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.

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

[1] Publication NIST SP800-53

catégorisation des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des actifs 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 devrait être effectuée par le détenteur de l'actif.

ARTICLE 7 : 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 politique de sécurité de l'information du Cégep se base sur cinq axes fondamentaux de gestion.

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 Cégep soient strictement réservés aux personnes autorisées afin de protéger la confidentialité.

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.

Gestion du risque

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

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 Cégep peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'actif informationnel.

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 l'institution financière tels les catastrophes naturelles, les pannes d'électricité ou de télécommunication, les pannes informatiques, le piratage, le terrorisme, les pandémies, etc. L'identification de ces incidents permet d'évaluer leurs impacts sur les activités de l'institution et de mettre en place les mesures d'atténuation nécessaires afin d'assurer la continuité des activités critiques.

ARTICLE 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, les membres de la communauté du Cégep doivent être sensibilisés :
- À la sécurité de l'information et des systèmes d'information du Cégep ;
- Aux conséquences d'une atteinte à la sécurité ;
- À leurs rôles et à leurs responsabilités en la matière.

Le Cégep 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. L'utilisatrice et l'utilisateur ont la responsabilité de participer à ces activités de sensibilisation et de formation. Par ailleurs, le Cégep favorise le recours aux services communs de formation en sécurité de l'information.

ARTICLE 9 : RÉVISION DE LA POLITIQUE

La politique sera révisée au besoin, au minimum tous les 3 ans à compter de sa date d'adoption.

ARTICLE 10 : ENTRÉE EN VIGUEUR DE LA POLITIQUE

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration. Elle abroge et remplace la Politique de Sécurité de l'information, d'utilisation des ressources informationnelles et de protection des renseignements personnels AG-18-PO-11.

ARTICLE 11 : 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.

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l'information qui en découlent, s'expose à 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.

De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au Cégep ou en vertu des dispositions de la législation applicable en la matière.