POL-15 Politique sur la sécurité de l'information

Adoptée par le Conseil d'administration le 25 septembre 2017

Adoption de la version révisée par le Conseil d'administration le 10 juin 2024

TABLES DES MATIÈRES

PRÉAMBULE ……..3
ARTICLE 1. OBJECTIFS 3
ARTICLE 2. PRINCIPES DIRECTEURS 4
ARTICLE 3. CADRE DE RÉFÉRENCE 4
ARTICLE 4. CHAMP D'APPLICATION 5
ARTICLE 5. DÉFINITIONS 5
ARTICLE 6. CADRE DE GESTION (CG) 6
6.1. Gestion des identités et des accès (GIA) 7
6.2. Gestion du risque 7
6.2.1 Prise en charge 7
6.2.2 Principes applicables 7
6.2.3 Analyse de risque 8
6.3. Gestion de la reprise et de la continuité des affaires 8
ARTICLE 7. RÔLES ET RESPONSABILITÉS 8
7.1. Conseil d'administration (CA) 8
7.2. Direction générale (DG) 9
7.3. Équipe de direction générale (ÉDG) 9
7.4. Direction des technologies informatiques (DTI) 9
7.5. Cheffe ou chef de la sécurité de l'information organisationnelle (CSIO) 10
7.6. Coordonnatrice organisationnelle ou coordonnateur organisationnel ou des mesures de sécurité de l'information (COMSI) 11
7.7. Responsable de l'accès à l'information et de la protection des renseignements personnels 11
7.8. Personnes répondantes en matière de sécurité de l'information 11
7.9. Direction des finances (DF) 12
7.10. Direction des ressources humaines et des affaires corporatives (DRHAC) 12
7.11. Responsable d'actifs informationnels 12
7.12. Personne utilisatrice des actifs informationnels 13
ARTICLE 8. SENSIBILISATION ET INFORMATION 13
ARTICLE 9. SANCTIONS 14
ARTICLE 10. RESPONSABLE DE L'APPLICATION 14
ARTICLE 11. RESPONSABLE DE LA DIFFUSION 14
ARTICLE 12. ENTRÉE EN VIGUEUR 14
ARTICLE 13. ABROGATION ET REMPLACEMENT 14
ARTICLE 14. RÉVISION 14

PRÉAMBULE

La présente *Politique sur la sécurité de l'information* (POL-15) (*Politique* 15) permet au Cégep Garneau (« Cégep ») d'accomplir sa mission, de préserver sa réputation, de respecter les lois et règlements, ainsi que de réduire les risques en protégeant l'information qu'il a créée ou reçue et dont il est responsable d'agir à titre de gardien.

Cette information est multiple et diversifiée. Y sont notamment inclus : les renseignements personnels des personnes étudiantes et des membres du personnel, l'information professionnelle sujette à des droits de propriété intellectuelle et l'information stratégique ou opérationnelle pour l'administration du Cégep.

À cet effet, la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (« LGGRI ») et la *Directive sur la sécurité de l'information gouvernementale* (« *Directive* ») viennent notamment établir les obligations des établissements collégiaux en leur qualité d'organismes publics.

Également, la *Directive* oblige le Cégep à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une *Politique sur la sécurité de l'information*, en ayant recours, notamment, à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

C'est dans ce contexte que le Cégep se dote de la présente *Politique* 15 visant à orienter et à renforcer les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois, règlements et directives gouvernementales, ainsi qu'aux autres besoins du Cégep en matière de réduction du risque associé à la protection de l'information.

ARTICLE 1. OBJECTIFS

Les objectifs qui sous-tendent la présente *Politique* 15 sont les suivants :

- affirmer l'engagement du Cégep à s'acquitter de ses obligations à l'égard de la sécurité de l'information afin de garantir et de répondre aux objectifs de sécurité de l'information, et ce, quel que soit son support ou ses moyens de communication ;

- 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 ;

- 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.

ARTICLE 2. PRINCIPES DIRECTEURS

Les principes directeurs qui sous-tendent la présente *Politique* 15 et qui guident les actions du Cégep en matière de sécurité de l'information sont les suivants :

- identifier l'information à protéger, ses caractéristiques de sécurité et désigner les personnes qui en sont responsables ;

- s'appuyer sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires ;

- adhérer à une approche basée sur le risque acceptable ;

- protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle jusqu'à sa destruction éventuelle ;

- mettre en place une gestion de la sécurité de l'information qui répond au changement constant de l'environnement technologique ;

- évaluer régulièrement les risques, mettre en place des mesures proactives de sécurité et des méthodes de détection d'usage abusif ou inapproprié de l'information, définir des actions d'éradication des menaces ou de recouvrement des activités compromises ;

- adhérer aux principes de partage des meilleures pratiques et de l'information opérationnelle en matière de sécurité de l'information avec le réseau de l'éducation et les organismes publics ;

- adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle ;

- s'assurer que chaque personne employée par le Cégep ait uniquement accès à l'information pertinente pour la réalisation de ses tâches normales ;

- s'assurer d'une communication efficace dans les situations pouvant affecter les actifs informationnels et être identifiées comme des menaces ;

- mettre en place un plan de continuité des affaires en vue de rétablir les services essentiels.

ARTICLE 3. CADRE DE RÉFÉRENCE

La présente *Politique* 15 est instituée en tenant compte, notamment du cadre de référence suivant :

- la *Charte des droits et libertés de la personne*, RLRQ, c. C-12 ;
- le *Code civil du Québec,* c. CCQ-1991 ;
- le *Code criminel*, LRC (1985) c. C-46 ;

- la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, RLRQ, c. G-1.03 et ses règlements ;
- la *Directive gouvernementale sur la sécurité de l'information,* Secrétariat du Conseil du Trésor, 8 décembre 2021 ;
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*, Secrétariat du Conseil du Trésor, 2012 ;
- la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1 ;
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1 et ses règlements ;
- la *Loi sur les archives*, L.R.Q. c. A-21.1 ;
- la *Loi sur le droit d'auteur*, RLRC, 1985, c. C-42 ;
- le *Règlement sur la protection des renseignements personnels*, R-07 ;
- le *Règlement concernant la gestion intégrée des documents du Cégep Garneau*, R-11 ;
- la *Procédure de traitement d'un incident de confidentialité,* PROC-21 ;
- le *Code de conduite des utilisateurs des actifs informationnels* ;
- Document ITSG-33 du gouvernement du Canada.

ARTICLE 4. CHAMP D'APPLICATION

La présente *Politique* 15 s'applique aux utilisatrices et aux utilisateurs de l'information, tels que définis à l'article 5.

L'information visée est celle que le Cégep détient dans le cadre de sa mission, et ce, que sa conservation soit assurée par lui-même ou par un tiers.

Tous les supports d'information, incluant le papier, sont concernés.

ARTICLE 5. DÉFINITIONS

Dans la présente *Politique* 15, à moins que le contexte ne s'y oppose, les mots suivants sont définis comme suit :

a) **Actif informationnel :** 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 (logiciels, progiciels, didacticiels, banques 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.

b) **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.

c) **Cadre de gestion :** l'ensemble des consignes qu'elles soient les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues qui encadrent les activités d'un établissement d'enseignement tel que le Cégep.

d) **Communauté étudiante :** toute personne qui fréquente le Cégep pour y étudier ou suivre une formation.

Y sont inclus notamment : toutes les personnes étudiantes, ainsi que les personnes participantes de la formation continue.

e) Confidentialité : la propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

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

g) Événement de sécurité : un 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.

h) Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni altérée, ni détruite sans autorisation.

i) Personne utilisatrice des actifs informationnels : tout membre du personnel et toute personne physique ou morale qui utilise les actifs informationnels du Cégep.

Y sont notamment inclus : une personne employée, une personne étudiante, une personne consultante, la clientèle de différents services, les personnes sous-traitantes, les fournisseuses et fournisseurs, les partenaires, les personnes accompagnatrices, les personnes invitées, le personnel des corporations affiliées au Cégep, ainsi que la Fondation du Cégep Garneau et son personnel.

j) Plan de continuité : l'ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité du Cégep.

k) Responsable d'actifs informationnels : le membre du personnel-cadre au sein d'une unité pédagogique ou administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité.

l) Risque de 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.

ARTICLE 6. CADRE DE GESTION (CG)

La *Politique* 15 du Cégep s'articule autour des trois axes fondamentaux de gestion suivants :

1. la gestion des identités et des accès (GIA) ;

2. la gestion du risque (GMVI) ;
   - la gestion des menaces ;
   - la gestion des vulnérabilités ;
   - la gestion des incidents.

3. la gestion de la reprise et de la continuité des affaires.

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 également de l'évolution des menaces et des risques.

6.1. Gestion des identités et des accès (GIA)

Afin de protéger la confidentialité de l'information, la GIA 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.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et sur l'imputabilité des personnes, à tous les niveaux de personnel du Cégep.

6.2. Gestion du risque

La gestion des risques touchant l'actif informationnel du Cégep s'appuie sur une analyse des menaces, des vulnérabilités et des incidents encourus reliés à l'intégrité, la disponibilité et la confidentialité de l'information détenue par le Cégep.

Basée sur une catégorisation des actifs informationnels à jour, cette analyse permet de connaître la valeur de l'information à protéger.

Conformément au processus de gestion des menaces, des vulnérabilités et des incidents (GMVI) du Centre gouvernemental de cyberdéfense, ce processus vise à normaliser la détermination des niveaux de coordination des incidents et l'implication des intervenants appropriés, ainsi que des modalités de prise en charge, de gestion et d'escalade des menaces, des vulnérabilités et des incidents.

6.2.1 Prise en charge

La prise en charge des menaces, des vulnérabilités et des incidents (MVI) peut nécessiter l'intervention de plusieurs intervenants, ainsi qu'une coordination adéquate entre eux.

Le processus GMVI a donc pour objectifs :

- de permettre une prise en charge cohérente et uniforme des MVI dans tous les organismes publics (OP) ;
- de mettre en place une méthode uniforme au sein du gouvernement pour traiter des situations qui dépassent les préjudices sectoriels et qui nécessitent d'être escaladées à un niveau supérieur ;
- de préciser les niveaux de coordination et les communications applicables à la prise en charge des MVI ;
- de définir un processus d'escalade des MVI clair et rapide ;
- d'améliorer la concertation entre les différentes instances gouvernementales ;
- d'harmoniser le processus organisationnel de gestion des MVI de chaque OP ;
- d'optimiser l'utilisation des ressources spécialisées.

6.2.2 Principes applicables

Le processus GMVI s'appuie sur les principes suivants :

- proposer une approche intégrée de la gestion des MVI à l'échelle gouvernementale ;

- s’inspirer des meilleures pratiques dans le domaine, dont le *Cadre de Cybersécurité* (CSF) du National Institute of Standards and Technology (NIST) ;

- s’appuyer sur les communautés de concertation en cybersécurité, définies dans la *Directive* et dans le *Cadre de gestion gouvernementale en sécurité de l’information* (« *Cadre* »), afin d’assurer des communications fluides entre les divers intervenants ;

- définir les rôles et les responsabilités du personnel et des instances au Cégep, et ce, en conformité avec les lois et règlements en vigueur ;

- introduire quatre (4) niveaux de coordination et en déterminer la personne ou l’instance responsable ;

- fixer le niveau de coordination par une approche axée sur le niveau d’impact du préjudice envers le citoyen, l’institution ou le gouvernement ;

- assurer une amélioration continue du processus GMVI.

6.2.3 Analyse de risque

L'analyse de risques guide également l'acquisition, le développement et l’exploitation des systèmes d’information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l’environnement du Cégep. La gestion des risques liés à la sécurité de l’information s’inscrit dans le processus global de gestion des risques du Cégep.

Les risques à portée gouvernementale doivent être déclarés conformément à la *Directive*.

Le niveau de protection de l’information est établi en fonction :

- de la nature de l’information et de son importance ;

- des probabilités d’accident, d’erreur ou de malveillance, auxquels elle est exposée ;

- des conséquences de la matérialisation de ces risques ;

- du niveau de risque acceptable par le Cégep.

6.3. 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, notamment les catastrophes naturelles, les pannes d’électricité ou de télécommunication, les pannes informatiques et le piratage.

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 7. RÔLES ET RESPONSABILITÉS

La présente *Politique* 15 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.

7.1. Conseil d’administration (CA)

Le CA assume les rôles et responsabilités suivants :

- adopter la présente *Politique* 15 ainsi que toute modification à celle-ci ;

- être régulièrement informé des actions du Collège en matière de sécurité de l'information.

7.2. Direction générale (DG)

La DG assume les rôles et responsabilités suivants :

- veiller à l'application de la présente *Politique* 15 ;

- encadrer la cheffe ou le chef de la sécurité de l'information organisationnelle (CSIO) dans la réalisation de son mandat ;

- assurer le maintien d'un lien fonctionnel entre les personnes répondantes en matière de sécurité de l'information ;

- autoriser les redditions de comptes en matière de sécurité de l'information ;

- autoriser, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente *Politique* 15, d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission du Cégep. Le cas échéant, l'autorisation de cette dérogation doit être complétée à partir du formulaire prévu à cet effet et doit être consignée dans un registre des dérogations ;

- autoriser une enquête lorsqu'il y a ou pourrait y avoir transgression de la présente *Politique* 15.

7.3. Équipe de direction générale (ÉDG)

L'ÉDG assume les rôles et responsabilités suivants :

- déterminer des mesures visant à favoriser l'application de la *Politique* 15 et des obligations légales du Cégep en matière de sécurité de l'information ;

- approuver les orientations stratégiques en la matière ;

- approuver les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information ;

- définir des directives et des procédures qui viendront préciser ou soutenir l'application de la présente *Politique* 15.

7.4. Direction des technologies informatiques (DTI)

La DTI assume les rôles et responsabilités suivants :

- accompagner les gestionnaires du Cégep dans la mise en application de la présente *Politique* 15 ;

- assurer la sécurité des technologies de l'information en déployant les mesures nécessaires et appropriées ;

- élaborer et mettre en œuvre des activités de sensibilisation à la sécurité de l'information pour les membres du personnel et les membres de la communauté étudiante du Cégep en collaboration avec la Direction des ressources humaines et des affaires corporatives (DRHAC) ;

- procéder, deux (2) fois par année, à une reddition de comptes en matière de sécurité de l'information auprès du CA ;

- déposer le bilan de sécurité annuel au CA concernant l'application de la présente *Politique* 15.

En outre, en matière de sécurité de l'information, la DTI s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels elle intervient, et pour ce faire :

- participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre, et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information ;

- s'assure de l'application du processus de Gestion des menaces, des vulnérabilités et des incidents du centre gouvernemental de cyberdéfense ;

- participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente *Politique* 15 et autorisées par la direction générale.

7.5. Cheffe ou chef de la sécurité de l'information organisationnelle (CSIO)

Un membre du personnel-cadre de la DTI est nommé à titre de personne CSIO conformément à l'article 7.8 de la présente *Politique* 15. Celle-ci relève de la direction générale.

La personne CSIO assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein du Cégep et travaille, en étroite collaboration, avec les personnes répondantes en matière de sécurité de l'information pour assurer la prise en charge des exigences de sécurité de l'information.

La personne CSIO assume, dans l'organisation fonctionnelle de la sécurité de l'information, les rôles et responsabilités suivants :

- 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 coordonne l'exécution et veille 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 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 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 modalités précisées par le CDSI ;

- fournir les informations demandées par le CGSI et le 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.

7.6. Coordonnatrice organisationnelle ou coordonnateur organisationnel ou des mesures de sécurité de l'information (COMSI)

La personne COMSI est responsable de l'application du processus de GMVI pour le Cégep et agit en soutien auprès de la personne CSIO.

En plus, elle assume les rôles et responsabilités suivants :

- représenter le Cégep et participer activement au Réseau d'alerte gouvernemental, coordonné par l'Équipe de réponse aux incidents de sécurité de l'information de l'Administration québécoise (le CERT/AQ) ;

- identifier 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.

7.7. Responsable de l'accès à l'information et de la protection des renseignements personnels

La personne responsable de l'accès à l'information et de la protection des renseignements personnels veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

À ce titre, elle assume les rôles et responsabilités suivantes :

- communiquer à la cheffe ou au chef de la sécurité de l'information organisationnelle (CSIO) les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles ;

- contribuer à assurer la cohérence et l'harmonisation des interventions avec la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels.

7.8. Personnes répondantes en matière de sécurité de l'information

Les personnes répondantes en matière de sécurité de l'information sont les suivantes :

- pour la sécurité informatique : la direction adjointe à la sécurité, à l'infrastructure et au développement des technologies de l'information ;

- pour la sécurité de l'information : la personne désignée à titre de CSIO ;

- pour la gestion des GMVI : la personne désignée à titre de COMSI ;

- pour les actifs informationnels du Cégep : la personne cadre détenant l'autorité au sein de chacune des Directions ou d'un service donné ;

- pour la protection des renseignements personnels : la personne responsable de l'accès à l'information et de la protection des renseignements personnels.

Ces personnes sont nommées par le CA du Cégep ou la DG, lorsque cette responsabilité lui est déléguée par résolution.

7.9. Direction des finances (DF)

La DF, en collaboration avec la personne CSIO, voit à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep.

7.10. Direction des ressources humaines et des affaires corporatives (DRHAC)

En matière de sécurité de l'information, la DRHAC obtient de toute nouvelle personne employée du Cégep, après lui en avoir montré la nécessité, son engagement au respect de la présente *Politique* 15.

7.11. Responsable d'actifs informationnels

La personne responsable d'actifs informationnels est la personne détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif, et dont le 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 peut donc y avoir plusieurs personnes responsables d'actifs informationnels dans un cégep.

La personne responsable d'actifs informationnels assume les rôles et responsabilités suivants :

- informer le personnel relevant de son autorité et les tiers avec lesquels transige le service, de la *Politique* 15 et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer ;

- collaborer activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques ;

- voir à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel autorisé en conformité avec la présente *Politique* 15 ;

- s'assurer que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et s'assurer que toute personne consultante, fournisseur ou fournisseuse, partenaire, personne invitée, organisme ou firme externe s'engage à respecter la présente *Politique* 15 ;

- rapporter à la DTI toute menace ou tout incident afférant à la sécurité de l'information ;

- collaborer à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'information ;

- rapporter à la personne CSIO tout problème lié à l'application de la présente *Politique* 15, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de cette *Politique* 15.

Toute personne responsable d'actifs informationnels peut déléguer une partie de sa responsabilité à une autre personne qui a des responsabilités de gestion au sein du service.

7.12. Personne utilisatrice des actifs informationnels

La responsabilité de la sécurité de l'information du Cégep incombe à toutes les personnes utilisatrices des actifs informationnels du Cégep.

Toute personne utilisatrice qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'elle en fait et doit procéder de manière à protéger cette information.

À cette fin, la personne utilisatrice assume les rôles et responsabilités suivants :

- se conformer à la présente *Politique* 15 et à toute autre directive du Cégep en matière de sécurité de l'information et d'utilisation des actifs informationnels et les respecter ;

- 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 de ses fonctions et aux fins auxquelles ils sont destinés ;
- respecter les mesures de sécurité mises en place, ne les contournent pas, ni modifient leur configuration ni les désactivent ;

- signaler au responsable du service ou du département, tout incident susceptible de constituer une contravention à la présente *Politique* 15 ou de constituer une menace à la sécurité de l'information du Cégep ;

- collaborer à toute intervention visant à indiquer ou à atténuer une menace à la sécurité de l'information ou à un incident de sécurité de l'information.

Aussi, toute personne utilisatrice doit, dans le cadre de ses activités professionnelles ou d'études, lorsqu'elle y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information, se conformer aux documents institutionnels, à savoir les règlements, politiques, procédures et directives en vigueur au Cégep.

ARTICLE 8. SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur la régulation des conduites 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 leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement.

De plus, des documents explicatifs sont disponibles sur le site Internet du Cégep.

ARTICLE 9. SANCTIONS

Toute personne utilisatrice des actifs informationnels qui contrevient aux cadres légaux, réglementaires et administratifs, à la présente *Politique* 15, ainsi qu'aux mesures de sécurité de l'information qui en découlent et/ou qui, par négligence ou par omission, fait en sorte que l'information n'est pas protégée adéquatement, engage sa responsabilité personnelle et s'expose à des sanctions.

La sanction appropriée est déterminée en fonction de la nature, la gravité et les conséquences de la contravention, et ce, en tenant compte des dispositions législatives, réglementaires et contractuelles applicables.

ARTICLE 10. RESPONSABLE DE L'APPLICATION

La DG est responsable de l'application de la présente *Politique* 15*.* Nonobstant ce qui précède, cette dernière peut déléguer cette responsabilité à la personne CSIO et à la DTI.

ARTICLE 11. RESPONSABLE DE LA DIFFUSION

La Direction des communications et des relations publiques (DCOMRP) est responsable de la diffusion de la présente *Politique* 15.

ARTICLE 12. ENTRÉE EN VIGUEUR

La présente *Politique* 15 est adoptée par le Conseil d'administration et entre en vigueur dès son adoption.

ARTICLE 13. ABROGATION ET REMPLACEMENT

La présente *Politique* 15 abroge le *Cadre de gestion de la sécurité de l'information* et remplace toute politique antérieure.

ARTICLE 14. RÉVISION

La présente *Politique* 15 est mise à jour lorsque l'évolution des cadres sociaux, administratifs, normatifs et juridiques le commande et minimalement tous les cinq (5) ans.