



## Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information

---



Recommandée par le Comité des orientations technologiques  
Adoptée par le Conseil d'administration le 17 février 2015  
Résolution : 2015-CA01-07

**Table des matières**

<b>1 - Définitions</b> .....	<b>3</b>
<b>2 - Préambule</b> .....	<b>3</b>
<b>3 - Objectifs</b> .....	<b>4</b>
3.1 Protéger l'actif informationnel du Cégep .....	4
3.2 Appliquer de bonnes pratiques de sécurité .....	4
3.3 Responsabiliser les personnes utilisatrices .....	4
<b>4 - Champ d'application</b> .....	<b>4</b>
<b>5 - Principes et règles d'application</b> .....	<b>4</b>
5.1 Propriété des données .....	4
5.2 Protection physique des actifs informationnels .....	4
5.3 Utilisation des actifs informationnels .....	5
5.3.1. Postes de travail .....	5
5.3.2. Systèmes d'information institutionnels, serveurs et réseaux locaux .....	5
5.3.3. Déplacement des équipements.....	5
5.3.4. Disposition de matériel et d'information .....	5
5.3.5. Prise de copie de sécurité .....	5
5.3.6. Courrier et messagerie électronique .....	6
5.4 Conservation et rétention des données .....	6
5.5 Protection des renseignements confidentiels et stratégiques.....	6
5.6 Maintenance des applications et des processus d'exploitation .....	6
5.7 Signalement des incidents .....	6
5.8 Propriété intellectuelle .....	6
5.9 Sensibilisation et information.....	7
5.10 Expectative de vie privée .....	7
5.11 Droit de vérification.....	7
5.12 Plan de continuité et de relève informatique .....	7
5.13 Départ d'une personne utilisatrice.....	7
5.14 Absence prolongée d'un membre du personnel .....	9
5.15 Maintenance des comptes étudiants.....	9
5.16 Entente de confidentialité – entreprise et organisme .....	9
5.17 Code d'utilisation des technologies à la bibliothèque.....	9
<b>6 - Exceptions</b> .....	<b>10</b>
<b>7 - Dérogation</b> .....	<b>10</b>
<b>8 - Partage des responsabilités</b> .....	<b>10</b>
<b>9 - Références et sources</b> .....	<b>10</b>
9.1 Pratiques de gestion.....	10
9.2 Références .....	11
<b>10 - Évaluation de l'application et révision de la politique</b> .....	<b>11</b>

## 1 - Définitions

- Actif informationnel : Tout système ou équipement du Cégep fourni, pouvant être sa propriété ou loué, permettant le traitement, le transport et l'entreposage de toute forme de communication ou d'information, notamment, les équipements informatiques (poste de travail, ordinateur portable, imprimante, etc.), les réseaux de communication (Internet, réseau local, réseau sans fil, réseau étendu, etc.), les systèmes de téléphonie, les systèmes de vidéosurveillance et de télécommunication, le courrier électronique, les bases de données, les images numérisées, les vidéos, les applications informatiques et les progiciels ainsi que la documentation nécessaire à leur bon fonctionnement. L'actif informationnel inclut aussi toute forme de communication ou d'information inscrite sur support papier, électronique ou autre, produite, transmise ou reçue par une personne utilisatrice dans le cadre des opérations du Cégep.
- Personne utilisatrice : Toute personne autorisée par le Cégep à utiliser les services et les actifs informationnels, notamment, les étudiantes et les étudiants, les membres du personnel enseignant (enseignement ordinaire et formation continue), les membres du personnel administratif (personnel de soutien, personnel professionnel, personnel cadre et hors-cadre), les personnes utilisatrices des services du Cégep, les fournisseurs, etc.
- Accessibilité des données : Mise à la disposition, sous diverses sources et médias, des actifs informationnels aux personnes utilisatrices et aux organismes ayant des liens avec le Cégep dans le cadre de ses opérations.
- Confidentialité des données : Consiste à assurer que les actifs informationnels soient accessibles seulement à celles et ceux dont l'accès est autorisé.
- Intégrité des données : État des données qui, lors du traitement, de la conservation ou de la transmission ne subissent aucune altération, destruction volontaire ou accidentelle et conservent leur format original permettant l'utilisation prévue.
- Poste de travail : Ordinateur du Cégep utilisé par une seule personne utilisatrice à la fois.
- Continuité informatique : Actions et procédés compensatoires visant à rétablir un service informatique affecté par une panne.
- Relève informatique : Actions et procédés compensatoires visant à rétablir les services informatiques les plus critiques affectés par une panne majeure pouvant nécessiter l'utilisation de sites externes.

Les sigles suivants sont utilisés dans le document pour en faciliter la lecture :

- Cégep : Cégep Saint-Jean-sur-Richelieu, incluant tous ses sites opérationnels
- DCAC : Direction des communications et des affaires corporatives
- SIM : Service de l'informatique et du multimédia
- TI : Technologies de l'information

## 2 - Préambule

Le Cégep Saint-Jean-sur-Richelieu reconnaît l'importance pour les membres du personnel et la population étudiante d'avoir accès à des actifs informationnels afin de réaliser des activités d'enseignement, de recherche, de gestion, d'administration et de service, en lien avec la mission de l'institution.

En tant que propriétaire et gestionnaire d'actifs informationnels et de renseignements personnels, le Cégep a la responsabilité légale d'assurer que l'utilisation, le traitement et la sécurité de ces derniers soient conformes à la présente politique, et ce, afin d'assurer le bon fonctionnement des activités et la réalisation de la mission du Cégep.

## 3 - Objectifs

### 3.1 Protéger l'actif informationnel du Cégep

La sécurité concernant les technologies de l'information au sein du Cégep vise à permettre la tenue de toutes les activités, notamment administratives et pédagogiques, en considérant la confidentialité, l'intégrité et l'accessibilité de tous les éléments de l'actif informationnel du Cégep.

### 3.2 Appliquer de bonnes pratiques de sécurité

Les mesures de protection de l'actif informationnel respectent les pratiques de gestion reconnues dans le domaine des technologies de l'information. Ces pratiques sont documentées par des directives et des procédures et sont sujettes à des révisions périodiques.

### 3.3 Responsabiliser les personnes utilisatrices

La protection de l'actif informationnel exige la contribution de toutes et de tous. Le Cégep informe et sensibilise les personnes utilisatrices afin qu'elles respectent et contribuent à la gestion sécuritaire et responsable de l'actif informationnel.

## 4 - Champ d'application

La présente politique s'applique :

- Aux membres du personnel régulier et occasionnel du Cégep, à la population étudiante tant à l'enseignement ordinaire qu'à la formation continue et aux personnes ou organismes utilisateurs (notamment des entreprises et des organismes communautaires) des actifs informationnels du Cégep;
- À tout l'actif informationnel appartenant au Cégep ou étant sous sa responsabilité;

et ce, dans le respect des lois en vigueur et du cadre réglementaire qui régissent le Cégep.

## 5 - Principes et règles d'application

Plus spécifiquement, la Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information est fondée sur les principes suivants :

### 5.1 Propriété des données

Le Cégep est propriétaire de toutes les données contenues sur les actifs informationnels qu'il utilise. Le Cégep peut être propriétaire ou locataire de ces actifs informationnels, par exemple des supports d'information ou des systèmes informatisés.

Le Cégep offre un espace de stockage sur les actifs informationnels (réseaux, appareils, systèmes), mais ne peut être tenu responsable de la perte de ces données.

Exclusions :

- À moins d'ententes contraires, toutes les réalisations pédagogiques ou de recherche des membres du personnel enseignant en sont leur propriété et sont régies par la convention collective du personnel enseignant. Il est de la responsabilité de ces derniers de conserver une copie de sécurité de leurs réalisations sur des supports personnels.
- Les réalisations pédagogiques des étudiantes et étudiants.
- Les boîtes courriel destinées aux syndicats et associations. Il est recommandé que ces derniers effectuent une copie de sauvegarde de leurs courriels.

### 5.2 Protection physique des actifs informationnels

Le Cégep, conformément aux pratiques dans le domaine des TI, met en place et maintient des moyens de sécurité et de contrôle afin d'empêcher tout dommage ou utilisation non autorisée des actifs informationnels.

### 5.3 Utilisation des actifs informationnels

- Les actifs informationnels publics (classes, laboratoires, bibliothèque et autres) doivent être utilisés qu'à des fins pédagogiques.
- Les actifs informationnels présents dans les bureaux des membres du personnel doivent être utilisés que dans le cadre des fonctions des personnes utilisatrices.
- Les actifs informationnels ne peuvent en aucun cas être utilisés pour archiver, enregistrer, distribuer ou éditer des documents portant atteinte à autrui ou à l'image du Cégep conformément au Règlement numéro 17 Relatif à la qualité des conditions de vie au Cégep.
- Le SIM s'assure que chaque personne utilisatrice ait accès aux ressources informationnelles nécessaires pour exercer ses fonctions pourvu que ces besoins respectent la sécurité et la bonne gestion des actifs informationnels. Ces droits sont validés régulièrement.
- L'utilisation des actifs informationnels est un privilège et non un droit. Ce privilège peut être révoqué en tout temps.

#### 5.3.1. Postes de travail

- Tous les postes de travail du Cégep comportent des mesures de protection contre les accès non autorisés et les vulnérabilités logicielles (logiciels malveillants, virus et autres).
- Tous les accès et privilèges sont régis par des codes utilisateurs et des mots de passe personnels.
- Tous les postes de travail achetés par le Cégep sont configurés, installés, maintenus à jour et reliés à son réseau.
- Les actifs informationnels, propriété du Cégep, peuvent être modifiés, remplacés, déplacés et retirés par le SIM selon les besoins de l'établissement et à la suite d'un préavis raisonnable.
- L'attribution et la gestion des droits de configuration des équipements du Cégep sont la responsabilité exclusive du SIM.
- Le SIM peut interdire l'accès au réseau du Cégep à tout poste de travail ou équipement qu'il juge non conforme.
- Aucune copie de sécurité des disques locaux n'étant effectuée, le Cégep n'est pas responsable de la perte de ces données.

#### 5.3.2. Systèmes d'information institutionnels, serveurs et réseaux locaux

- Tout système d'information institutionnel doit être protégé, au minimum, par un processus d'accès nécessitant un mécanisme de codes et de mots de passe. Il doit, en plus, limiter cet accès aux personnes autorisées seulement, en fonction de la nature de l'information et des applications utilisées.
- Chaque personne utilisatrice obtient un compte unique qui l'identifie.
- Les personnes utilisatrices ne doivent pas entraver le fonctionnement des outils de sécurité tels que l'antivirus, les sauvegardes de données, les écrans de veille et les outils de contrôle d'accès.
- Il est de la responsabilité du propriétaire du compte utilisateur de conserver de façon confidentielle le mot de passe qui y est rattaché et de prendre les mesures nécessaires pour le protéger.

#### 5.3.3. Déplacement des équipements

Seuls les membres du personnel du SIM ou les personnes autorisées par le SIM, peuvent déplacer et installer des équipements informatiques, téléphoniques, réseautiques et de multimédias fixes.

Le déplacement d'équipements hors des locaux du Cégep doit être autorisé par le SIM. Il est de la responsabilité de la personne utilisatrice d'assurer la sécurité et la protection de ces équipements.

#### 5.3.4. Disposition de matériel et d'information

Seul le SIM est dûment autorisé à disposer des équipements présents dans l'actif informationnel. Cette opération, réalisée en collaboration avec le Service des approvisionnements, doit privilégier une méthode de recyclage et de mise au rebut sécurisée et respectueuse de l'environnement.

Tout équipement inutilisé doit être signalé au SIM pour récupération. Les équipements ainsi récupérés deviennent disponibles dans l'inventaire du Cégep et pourront être redistribués selon les besoins de l'ensemble des services et départements.

#### 5.3.5. Prise de copie de sécurité

- Toute information hébergée sur un serveur du Cégep fait l'objet d'une sauvegarde de sécurité quotidienne.
- Les supports utilisés pour effectuer des copies sont conservés selon les pratiques du domaine des TI.
- Les activités de sauvegarde de sécurité sont conformes aux règles du calendrier de conservation établi au Cégep.

## Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information

---

### 5.3.6. Courrier et messagerie électronique

Dans le but de lutter contre la propagation et l'exécution de codes malveillants, l'interception d'informations sensibles, la désinformation, le pollupostage (*spamming*) et la publication d'informations illégales, diffamatoires ou de harcèlement, le Cégep établit les règles suivantes quant à l'utilisation de ses systèmes de courriel.

Pour tout message électronique transmis à partir du réseau du Cégep, la personne utilisatrice doit :

- Respecter, lorsqu'il y a lieu, la confidentialité des messages diffusés.
- Ne supprimer et ne conserver aucune trace des messages ne lui étant pas destinée.
- Se conformer à la directive de la Direction générale en vigueur concernant l'envoi massif de courriels.
- Faire preuve de vigilance en évitant d'ouvrir un courrier électronique de provenance inconnue ou douteuse.

### 5.4 Conservation et rétention des données

Toute donnée recueillie des systèmes informatisés est conservée de façon sécuritaire, détruite ou mise au rebut selon les règles de conservation des données, élaborées dans le calendrier de conservation disponible dans le « Recueil des délais de conservation des documents administratifs du Cégep Saint-Jean-sur-Richelieu » et spécifié en conformité avec les dispositions de la *Loi québécoise sur les archives*.

### 5.5 Protection des renseignements confidentiels et stratégiques

- Toute information considérée confidentielle ou stratégique est protégée contre tout accès ou utilisation non autorisés ou illicites.
- Les renseignements détenus par le Cégep sont utilisés et servent uniquement aux fins pour lesquelles ils ont été recueillis.
- La gestion de ces renseignements respecte la *Loi sur la protection des renseignements personnels*.

### 5.6 Maintenance des applications et des processus d'exploitation

- L'environnement servant à effectuer la maintenance des applications et des processus doit être isolé de l'environnement réel de production.
- L'acquisition, le développement et la maintenance des applications sont des choix stratégiques. Les applications ou les processus d'exploitation susceptibles d'entraîner des répercussions sur l'information critique du Cégep ne doivent être accessibles que par l'intermédiaire de moyens sécurisés dans un environnement contrôlé et restreint.
- Toute opération critique effectuée sur ou par l'intermédiaire d'une application ou d'un processus d'exploitation doit pouvoir être retracée par le personnel dûment habilité à l'aide de journaux d'événements sécurisés et préservés pour références futures.

Les ententes et les contrats entre le Cégep et des fournisseurs de biens et de services, tant pour l'acquisition, le développement et la maintenance des applications, doivent contenir des dispositions obligeant la signature de « L'entente de confidentialité ». Le contractant doit garantir son respect des standards de sécurité mentionnés.

### 5.7 Signalement des incidents

Il est de la responsabilité de toutes les personnes utilisatrices de signaler au SIM, dans les plus brefs délais, toute faille ou tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité de l'information.

### 5.8 Propriété intellectuelle

Les personnes utilisatrices doivent se conformer aux exigences de la *Loi sur le droit d'auteur du Canada* et les ententes intervenues entre le Cégep et les sociétés de gestion des droits d'auteur, notamment Copibec et la SOCAN. Il est de la responsabilité de toutes et tous de valider ses actions avant de procéder à tout acte relié à la propriété intellectuelle afin d'obtenir les droits d'utilisation.

## Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information

---

### 5.9 Sensibilisation et information

Le Cégep s'engage à sensibiliser et à informer les personnes utilisatrices des actifs informationnels et des mesures de sécurité informationnelle applicables.

### 5.10 Expectative de vie privée

Aucune personne utilisatrice à l'exception des associations et des syndicats, ne peut prétendre à l'aspect privé de son utilisation des actifs informationnels du Cégep.

### 5.11 Droit de vérification

Si le Cégep a des motifs raisonnables de croire qu'une personne utilisatrice commet une infraction à la présente politique ou à une loi, il pourra procéder à la mise en place de mesures de vérification ciblées. Ce droit de vérification sera exercé avec circonspection et sera limité à la vérification de l'infraction suspectée.

### 5.12 Plan de continuité et de relève informatique

Un plan de continuité et de relève informatique des actifs informationnels du Cégep est mis en place et fait l'objet de tests et de simulations périodiques en tout ou en partie par le SIM. Pour des raisons de sécurité, ce plan est confidentiel.

### 5.13 Départ d'une personne utilisatrice

Selon les circonstances et les motifs de départ d'une personne utilisatrice, des privilèges d'accès pourraient être suspendus. Le tableau suivant résume les différents scénarios :

Type de personne utilisatrice	Motif de départ	Modification de privilèges
Population étudiante Ordinaire et formation continue	Renvoi	Suspension immédiate des : <ul style="list-style-type: none"><li>▪ Accès réseau et répertoire</li><li>▪ Accès aux applications</li><li>▪ Accès au compte courriel et contenu</li><li>▪ Crédits d'impression</li></ul>
Population étudiante Ordinaire et formation continue	Fin de fréquentation du Cégep	Suspension dès la date de demande de révision de notes par l'étudiante ou l'étudiant : <ul style="list-style-type: none"><li>▪ Accès réseau et répertoire</li><li>▪ Accès aux applications</li><li>▪ Accès au compte courriel et contenu</li><li>▪ Crédits d'impression</li></ul>
Personnel enseignant	Congédiement	Suspension immédiate des : <ul style="list-style-type: none"><li>▪ Accès réseau et répertoire</li><li>▪ Accès aux applications</li><li>▪ Accès au compte courriel et contenu</li></ul>
Personnel enseignant	Démission / retrait de priorité	Suspension le lendemain de son départ : <ul style="list-style-type: none"><li>▪ Accès réseau et répertoire</li><li>▪ Accès aux applications</li><li>▪ Accès au compte courriel et contenu</li></ul>

## Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information

Type de personne utilisatrice	Motif de départ	Modification de privilèges
Personnel enseignant	Fin de contrat	<p>Suspension après trois sessions complètes (excluant l'été) consécutives sans contrat au Cégep :</p> <ul style="list-style-type: none"> <li>▪ Accès réseau et répertoire</li> <li>▪ Accès aux applications</li> <li>▪ Accès au compte courriel et contenu</li> </ul> <p>Un avis par courriel sera expédié minimalement deux semaines avant la fermeture.</p>
Personnel enseignant	Retraite	<p>Suspension le lendemain de son départ :</p> <ul style="list-style-type: none"> <li>▪ Accès réseau et répertoire</li> <li>▪ Accès aux applications</li> <li>▪ L'adresse courriel demeure active à vie. Les courriels entrants seront redirigés vers une adresse fournie par la personne.</li> </ul>
Personnel administratif	Congédiement	<p>Suspension immédiate des :</p> <ul style="list-style-type: none"> <li>▪ Accès réseau et répertoire</li> <li>▪ Accès aux applications</li> <li>▪ Accès au compte courriel et contenu</li> </ul>
Personnel administratif	Fin de contrat	<p>Suspension après 12 mois complets consécutifs sans contrat au Cégep :</p> <ul style="list-style-type: none"> <li>▪ Accès réseau et répertoire</li> <li>▪ Accès aux applications</li> <li>▪ Accès au compte courriel et contenu</li> </ul> <p>Un avis par courriel sera expédié minimalement une semaine avant la fermeture.</p>
Personnel administratif	Démission / Retrait de priorité	<p>Suspension le lendemain de son départ :</p> <ul style="list-style-type: none"> <li>▪ Accès réseau et répertoire</li> <li>▪ Accès aux applications</li> <li>▪ Accès au compte courriel et contenu</li> </ul>
Personnel administratif	Retraite	<p>Suspension le lendemain de son départ :</p> <ul style="list-style-type: none"> <li>▪ Accès réseau et répertoire</li> <li>▪ Accès aux applications</li> <li>▪ L'adresse courriel demeure active à vie. Les courriels entrants seront redirigés vers une adresse fournie par la personne.</li> </ul>
Communautaire (personne utilisatrice des services, n'étant ni un membre du personnel, ni un étudiant ou étudiante)	Après 18 mois d'inutilisation	<p>Suspension immédiate après 18 mois d'inutilisation :</p> <ul style="list-style-type: none"> <li>▪ Accès réseau</li> <li>▪ Accès aux applications</li> <li>▪ Crédit d'impression</li> </ul>



## Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information

Type de personne utilisatrice	Motif de départ	Modification de privilèges
Fournisseur	Fin de contrat	Suspension immédiate des : <ul style="list-style-type: none"><li>▪ Accès réseau et répertoire</li><li>▪ Accès aux applications</li><li>▪ Accès au compte courriel et contenu</li></ul>

Dans le cas d'un congédiement, le contenu de la boîte courriel et du répertoire personnel pourront être remis au gestionnaire.

Dès l'annonce d'une démission, d'une fin de contrat, d'un retrait de priorité (personnel enseignant) ou d'une retraite, il est de la responsabilité du membre du personnel de remettre les courriels, les données (physiques et électroniques) pertinentes et les actifs informationnels qu'il a en sa possession à son gestionnaire. Sa boîte courriel et son espace personnel réseau devront être vidés.

Selon la situation, la direction du Cégep pourra demander au SIM d'effectuer une copie de sûreté des courriels et des données.

Après le départ de la personne utilisatrice, le Cégep ne remettra aucune donnée à celle-ci.

### 5.14 Absence prolongée d'un membre du personnel

L'absence prolongée est définie par une absence de plus de quatre semaines consécutives pour une raison différente que celle des vacances annuelles ou d'une fin de contrat.

Le compte courriel et les différents privilèges d'accès demeureront actifs pendant l'absence.

La personne utilisatrice doit conserver de façon confidentielle le mot de passe qui est rattaché à son compte réseau et son compte courriel.

À la demande de la personne utilisatrice ou à celle de la Direction des ressources humaines, les comptes utilisateurs réseau et courriel seront suspendus pendant une absence prolongée.

À la demande du gestionnaire, la personne utilisatrice devra remettre les actifs informationnels (ordinateur portable, cellulaire, etc.) qu'il a en sa possession.

### 5.15 Maintenance des comptes étudiants

Pour des raisons de maintenance des comptes étudiants, ces derniers pourraient ne pas être accessibles temporairement dans les périodes d'intersession. La population étudiante sera informée de ces modalités.

### 5.16 Entente de confidentialité – entreprise et organisme

Avant d'entreprendre une relation d'affaires avec le Cégep, les représentantes ou représentants autorisés de toute entreprise ou de tout organisme devront signer le document « Entente de confidentialité » assurant leur compréhension et leur acceptation des conditions décrites dans ledit document.

### 5.17 Code d'utilisation des technologies à la bibliothèque

Toute personne utilisatrice (n'étant pas une étudiante ou un étudiant inscrit ou un membre du personnel du Cégep) des services informatiques à la bibliothèque, devra signer et remettre au comptoir de la bibliothèque du Cégep le document « Code d'utilisation des technologies à la bibliothèque », assurant ainsi sa compréhension et son acceptation des conditions décrites dans ledit document.

### 6 - Exceptions

Des équipements et des locaux destinés à l'apprentissage technique et à la recherche, notamment en informatique et en réseautique, peuvent être en tout ou en partie exclus de certaines clauses de la présente politique. Ces exceptions, en accord avec le SIM, ne pourront remettre en question la sécurité de l'information et des technologies de l'information du Cégep.

### 7 - Dérogation

Les membres du personnel du Cégep peuvent demander une dérogation à l'application de certaines clauses de la politique. Ils doivent remplir le formulaire « Demande de dérogation », le faire approuver par leur gestionnaire et le retourner au SIM.

La coordination du SIM peut accepter ou rejeter toute demande de dérogation par la personne utilisatrice. Selon la nature de la demande, l'accord de la direction concernée pourra être nécessaire.

Dans le cas d'une absence prolongée, le membre du personnel pourra permettre l'accès à son compte courriel ou à ses données personnelles à une autre personne utilisatrice en remplissant et en signant le formulaire « Demande de dérogation » pour autoriser les accès. Advenant l'incapacité de ce dernier (maladie sévère, absence, etc.) d'autoriser cet accès, la Direction des ressources humaines pourra le faire.

### 8 - Partage des responsabilités

Des responsabilités additionnelles de la présente politique s'appliquent pour :

- La Direction générale  
La Direction générale est responsable de sa diffusion et de sa mise en œuvre. Elle s'assure que les objectifs et les principes en matière de sécurité de l'information sont connus et appliqués.
- La coordination du SIM  
Sous l'autorité immédiate de la Direction générale, la coordination du SIM agit comme premier intervenant à la sécurité des technologies de l'information. Cette dernière coordonne l'action des divers acteurs dans l'élaboration, la mise en place, le suivi et l'évaluation de la sécurité de l'information.
- Les directions et les coordinations de service  
Elles doivent informer et rappeler à leur personnel les responsabilités de chacune et chacun face à la présente politique.
- Les personnes utilisatrices  
Elles doivent connaître et respecter la présente politique.

### 9 - Références et sources

#### 9.1 Pratiques de gestion

Plusieurs pratiques de gestion reconnues dans le domaine des technologies de l'information existent. Dans le présent document, les pratiques suivantes ont été considérées :

- *ITIL (Information Technology Infrastructure Library)*
- *COBIT (Control Objective for information and related technology)*
- *ISO17799 (BS-77992) (Normes ISO en sécurité des TI)*

## Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information

---

### 9.2 Références

La Politique relative à la sécurité de l'information et à l'utilisation des technologies de l'information s'inspire de :

- Cégep de Sainte-Foy, Politique de sécurité de l'actif informationnel, 22 février 2010
- École de technologie supérieure, *Politique de sécurité de l'information*, 22 février 2007.
- Collège Lionel-Groulx, *Politique de sécurité informatique*, Collège Lionel-Groulx.
- Institut de sécurité informatique du Québec (ISIQ), *Modèle de politique de sécurité*, juillet 2007.
- Ville de Brossard, Politique de sécurité des technologies informatiques.
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1).
- La *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C-1.1).
- Conseil du trésor du Québec, la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI).
- Conseil du trésor du Québec, le *Guide d'utilisation du formulaire de bilan et de plan d'action de sécurité de l'information 2013-2014*, août 2014.
- MESRS, Encadrement de la sécurité de l'information gouvernementale pour le secteur de l'éducation, août 2014.
- Cégep Saint-Jean-sur-Richelieu, Calendrier de conservation (Recueil des délais de conservation des documents administratifs), mars 1997.

## 10 - Évaluation de l'application et révision de la politique

Le conseil d'administration peut procéder, au besoin, à l'évaluation de l'application de la politique ainsi qu'à sa révision.