Collège de Valleyfield
L'HISTOIRE • L'EXPÉRIENCE • LE SUCCÈS

Direction des affaires corporatives, du développement institutionnel et des communications

RECUEIL DE GESTION

TITRE: ***Politique de sécurité de l'information, d'utilisation des ressources informationnelles et de protection des renseignements personnels***

NUMÉRO : ***AG-18-PO-11***

Responsable de l'application

- [ ] *Président du conseil d'administration*
- [x] *Direction générale*
  - [ ] *Service 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 et approvisionnement*
  - [ ] *Service des ressources matérielles et des services communautaires*
  - [ ] *Service 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 Collège*

Approuvé par

- *Conseil d'administration*

Document de référence

Mise en application

- *Adoption : 12 juin 2018*
- *Entrée en vigueur : 12 juin 2018*
- *Révision : aucune*
- *Modification : aucune*

Article 1 – OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du Collège à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information et de la protection des renseignements personnels, quels que soient leurs supports ou leurs moyens de communication. Plus précisément, le Collège doit veiller à:

- La disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- L'intégrité de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- La confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

Par conséquent, le Collège 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.

La présente politique établit également les conditions d'utilisation des actifs informationnel par tout usager, de manière à :

- Promouvoir une utilisation responsable des actifs informationnels;
- Préserver la réputation du Collège comme établissement d'enseignement collégial responsable;
- Prévenir une utilisation abusive ou illégale des actifs informationnels;
- Délimiter les balises de la protection de la vie privée de l'usager dans l'utilisation des actifs informationnels;
- Fournir un cadre de référence déterminant les conditions d'utilisation des technologies de l'information et des communications.

Article 2 – CHAMP D'APPLICATION ET CADRE JURIDIQUE

La présente politique s'adresse à tous les usagers de la communauté collégiale, c'est-à-dire à toute personne physique ou morale qui, à titre de membre du personnel, de consultant, de partenaire, de fournisseur, de locataire, de syndicats, d'étudiant ou de public, utilise les actifs informationnels du Collège.

L'information visée est celle que le Collège détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

Tous les supports, incluant le papier, sont concernés.

Plusieurs comportements attendus des usagers, notamment mais non limitativement prévus aux articles 6.2., 7.2.1. et à la nétiquette du Collège de Valleyfield, s'appliquent avec adaptation lorsque les usagers utilisent dans leur vie personnelle ou professionnelle, au Collège ou ailleurs, des actifs informationnels du Collège.

La politique de sécurité s'inscrit principalement dans un contexte régi par :

- La Charte des droits et libertés de la personne (LRQ, chapitre C-12);
- Le Code civil du Québec (LQ, 1991, chapitre 64);
- La Politique-cadre sur la gouvernance et la gestion des actifs informationnels des organismes publics;
- La Loi sur la gouvernance et la gestion des actifs informationnels des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03);
- La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);

- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- La Loi sur les archives (LRQ, chapitre A-21.1);
- Le Code criminel (LRC, 1985, chapitre C-46);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2);
- La Directive sur la sécurité de l'information gouvernementale;
- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42).
- La Politique de communication du Collège;
- La Politique de valorisation de la langue française du Collège;
- Les licences et ententes de groupe signées par le Collège;
- Les lois fédérales, dont celles relatives à la pornographie juvénile, à l'obscénité et à toute forme de propagande haineuse;
- Les conventions collectives et les contrats de travail.

Les principaux extraits de codes et de lois ainsi que des références à des textes légaux en relation avec la présente politique se retrouvent en annexe A.

Article 3 – DÉFINITIONS

3.1 Accessibilité des données

Mise à la disposition, sous diverses sources et médias, des actifs informationnels aux usagers et aux organismes ayant des liens avec le Collège dans le cadre de ses opérations.

3.2 Actif informationnel

Tout système ou équipement du Collège 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 un support papier, électronique ou autre, produite, transmise ou reçue par un usager dans le cadre des opérations du Collège.

3.3 Collège

Le Collège de Valleyfield en tant que personne morale, ses lieux incluant tous ses sites d'opération.

3.4 Confidentialité des données

Consiste à assurer que les actifs informationnels soient accessibles seulement à celles et ceux dont l'accès est autorisé.

3.4 Relève et continuité informatique

Actions et procédés compensatoires visant à rétablir un ou des services informatiques affectés par une panne.

3.5 Droit d'auteur

Tout droit conféré par la Loi sur le droit d'auteur. Il s'agit notamment du droit exclusif du titulaire de ce droit de publier, produire, reproduire, représenter ou exécuter en public, par télécommunication ou autrement, de traduire ou d'adapter sous une autre forme son œuvre ou une partie importante de celle-ci, ou de permettre à quelqu'un d'autre de le faire. Poser l'un ou l'autre de ces gestes sans le consentement du titulaire du droit constitue une violation du droit d'auteur.

3.6 Droit d'utilisation

Autorisation accordée à une personne physique ou morale définissant l'usage qu'elle peut faire des actifs informationnels dans le respect de la politique et dans le cadre des activités rattachées à son statut ou à ses fonctions.

3.7 Étudiante ou étudiant

Toute personne inscrite officiellement à ce titre dans les registres du Collège, quel que soit son régime d'études.

3.8 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.

3.9 Journalisation

Action de relever dans un journal (log) tous les évènements qui se produisent dans un système. La journalisation permet d'effectuer des analyses diverses, généralement statistiques, de faire des hypothèses sur les dysfonctionnements ou les pertes de performance d'un système. Elle sert également à enregistrer et à établir l'utilisation des services qui est faite par l'usager, telle que la photocopie, la télécopie, la téléphonie, l'impression sur imprimantes, les adresses Internet consultées, les quantités de courriels entrants et sortants de l'usager, la quantité (flux) transitant sur les serveurs, etc.

3.10 Médias sociaux

Groupe d'applications en ligne qui se fondent sur la philosophie et la technologie du Web et permettent l'interaction, la création et l'échange de contenu généré par les utilisateurs, tel que du texte, des images et des vidéos. Les technologies comprennent notamment, les sites sociaux de réseautage (Facebook, My Space, Google +), les sites de partage de contenus (YouTube, Flickr, Instagram, Pinterest), les blogues et microblogues (WordPress, Tumblr, Twitter) les réseaux professionnels (LinkedIn), les forums et les wikis, les flux RSS et autres flux de syndication Web. Contrairement aux médias traditionnels, ce sont des lieux où les internautes peuvent créer et participer en temps réel à l'information.

3.11 Membre du personnel

Toute personne salariée syndiquée ou non, incluant les cadres et les hors cadres, les travailleurs et travailleuses autonomes, les sociétés en nom collectif sous contrat avec le Collège ainsi que les personnes retraitées du Collège.

3.12 Nétiquette

Ensemble des conventions de bienséance régissant le comportement des internautes, notamment lors des échanges dans les forums, les réseaux sociaux ou par courrier électronique.

3.13 Œuvre

Toute œuvre littéraire, dramatique, musicale ou artistique, une banque de données ou d'information (textuelle, sonore, symbolique ou visuelle), une prestation d'un spectacle ou toute autre œuvre visée par la Loi sur le droit d'auteur, que cette œuvre soit fixée sur un support conventionnel (livre, bande sonore, vidéocassette) ou sur un support informatique (clé USB, cédérom, logiciel, disque dur) ou accessible par Internet.

3.14 Poste de travail

Ordinateur du Collège utilisé par un seul usager à la fois.

3.15 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.

3.16 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.

3.17 Service des technologies de l'information (STI)

Équipe du Collège incluant le coordonnateur 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 Collège ou ailleurs.

3.18 Technologies de l'information et des communications (TIC)

Techniques et ressources utilisées dans le traitement ou la transmission d'informations et qui sont liées à l'informatique, à Internet et aux télécommunications.

3.19 Usager

Membre du personnel, étudiant jeune ou adulte, ainsi que toute personne physique ou morale appelée ou autorisée à utiliser les actifs informationnels du Collège.

Article 4 – PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du Collège en matière de sécurité de l'information et de protection des renseignements personnels sont les suivants :

- S'assurer de bien connaitre l'information à protéger, en identifier les responsables et leurs caractéristiques de sécurité;
- 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 la gestion du risque acceptable. La mise en place du cadre de gestion est un moyen d'ajuster le risque par une combinaison de mesures raisonnables mises en place pour garantir la sécurité de l'information à un coût proportionnel à la sensibilité de l'information et aux dommages potentiels;
- Protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;
- S'engager à utiliser de façon responsable les données collectées uniquement pour résoudre des incidents ou pour gérer les opérations administratives essentielles du Collège;
- Protéger l'information tout au long de son cycle de vie, c'est-à-dire de son acquisition ou de sa création jusqu'à sa destruction, le niveau de sécurité pouvant varier au cours du cycle de vie du document;
- Adhérer à une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle, chaque personne qui a accès à l'information étant responsable de respecter les critères de confidentialité, de disponibilité et d'intégrité de celle-ci;
- Communiquer de façon transparente au sujet des menaces pouvant affecter les actifs informationnels, afin que toute personne puisse comprendre l'importance d'appliquer la sécurité comme on le demande, être informée de telle sorte qu'elle puisse reconnaître les incidents de sécurité et agir en conséquence.

Article 5 – CADRE DE GESTION ET AXES FONDAMENTAUX

L'efficacité des mesures de sécurité de l'information exige l'attribution claire des rôles et des responsabilités aux différents acteurs du Collège, par la mise en place d'un cadre de gestion de la sécurité de l'information permettant notamment une reddition de comptes adéquate.

Le cadre de gestion vise à renforcer les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins du Collège en matière de réduction du risque associé à la protection de l'information. Le cadre de gestion consiste en **un ensemble de directives, règles et procédures permettant au Collège de s'acquitter des contrôles nécessaires en matière de protection de l'information**.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être remises en question 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 menaces et des risques.

La politique de sécurité de l'information et de protection des renseignements personnels du Collège ainsi que le cadre de gestion qui en découle s'articulent autour de trois axes fondamentaux de gestion : la gestion des accès, la gestion des risques et la gestion des incidents.

Article 6 – GESTION DES ACCÈS ET UTILISATION DES RESSOURCES INFORMATIONNELLES

La gestion des accès doit être encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de l'information soient strictement réservés aux personnes autorisées. Ces mesures sont prises dans le dessein de protéger l'intégrité et la confidentialité des données et des renseignements personnels.

6.1 Autorisation et protection de l'accès

Seules les personnes autorisées peuvent utiliser les actifs informationnels du Collège.

Tout usager possède un identifiant personnel (code d'accès et mot de passe) qui lui permet d'accéder à l'information et aux équipements auxquels il a droit. Par conséquent, l'usager :

- Doit s'identifier avec le code d'accès et le mot de passe qui lui sont attribués par le STI;
- Est responsable en tout temps de l'utilisation et de la protection de ses codes d'accès et de ses mots de passe, qui ne doivent pas être révélés à d'autres personnes;
- Est responsable des activités découlant de l'utilisation de ceux-ci;
- Modifie ses mots de passe selon la directive en vigueur au Collège;
- S'identifie clairement dans sa correspondance ou sur ses publications électroniques.

6.2 Règles d'utilisation des actifs informationnels

6.2.1 Restriction d'utilisation

Toute utilisation des actifs informationnels du Collège à des fins non autorisées ou illégales est strictement interdite.

Sont notamment interdits en tout temps :

- Tout acte pouvant nuire au bon fonctionnement des actifs informationnels informatiques, entre autres, par l'insertion ou la propagation de virus, par la destruction ou la modification non autorisée de données ou de logiciels, ou par des gestes visant à désactiver, défier ou contourner les systèmes de sécurité du Collège;
- L'utilisation des actifs informationnels à des fins commerciales (publicité, promotion ou transaction), autres que celles reliées aux activités du Collège ou autorisées par la direction du Collège;
- L'association de propos personnels au nom du Collège dans un des médias sociaux, dans un groupe de discussion ou dans une séance de clavardage de manière à laisser croire que ces opinions sont endossées par le Collège, sauf lorsque cela est fait par une personne autorisée à le faire dans l'exercice de ses fonctions conformément à la Politique de communications DC-08-PO-01;
- La participation à des jeux collectifs dans Internet sauf si cette participation s'inscrit dans le cadre d'une activité en lien avec la mission du Collège ou encore si elle est autorisée par le Collège;
- L'accès, sans autorisation préalable de la direction, à des services ou à des banques de données pour lesquels des frais seraient facturés au Collège;
- Le téléchargement, le stockage ou la diffusion de documents qui ne sont pas en lien avec une activité d'enseignement ou le travail d'un usager (ex. films, logiciels, jeux, musique, etc.), ou

sinon, autorisés préalablement par la direction, la diffusion devant respecter, entre autres, le droit d'auteur;

- La consultation des sites véhiculant de l'information de nature violente, raciste, haineuse, homophobe, pornographique ou des sites de jeux, de paris ou de concours non autorisés, à moins que cela soit en lien direct avec une activité d'enseignement ou le travail d'un usager;
- Le téléchargement, le stockage ou la diffusion de fichiers contenant des propos ou des images ne respectant pas la Charte des droits et libertés de la personne, le droit à la vie privée ou toute autre loi ou règlement;
- La diffusion des messages répétitifs visant ou ayant pour effet d'encombrer un site à partir des équipements du Collège;
- L'utilisation des actifs informationnels à des fins de plaisanterie de mauvais goût, de harcèlement ou de menace sous quelque forme que ce soit;
- La participation à des chaines de lettres ou à des envois massifs à des fins personnelles (ex. ventes, sollicitations à des fins politiques, etc.), et ce, sans autorisation explicite;
- La modification, la destruction ou l'installation des configurations, des programmes ou des logiciels ou encore des composantes matérielles aux ordinateurs, aux périphériques ou aux appareils de télécommunications;
- L'utilisation des actifs informationnels, des communications et de l'Internet de manière à causer des anomalies ou des pannes dans les systèmes ou dans les réseaux auxquels il a accès (piratage, intrusion, blocage, etc.) ou de manière à bloquer l'accès à d'autres personnes;
- Le vol, le plagiat, la destruction ou la modification des données appartenant à un tiers;
- La recherche dans le but de s'approprier le code d'accès et le mot de passe d'un tiers;
- Le cryptage des données sans fournir les codes d'accès au Service de l'informatique à la suite d'une demande en ce sens;
- L'accès ou les tentatives d'accès à des données, à des fichiers ou à des réseaux auxquels l'usager n'a pas été autorisé préalablement;
- L'utilisation excessive ou impertinente qui entraine la surcharge des réseaux;
- Toute autre manipulation des actifs informationnels contraire à l'esprit de la politique.

6.2.2 Utilisation raisonnable

L'utilisation des actifs informationnels doit être raisonnable afin de permettre l'accès à tous les usagers et d'en assurer la durabilité. Dans un contexte de partage des ressources, l'usager ne doit pas monopoliser ou abuser des actifs informationnels.

6.2.3 Postes de travail

Tous les postes de travail achetés par le Collège sont configurés, installés, maintenus à jour et reliés à son réseau. Ils comportent des mesures de protection contre les accès non autorisés et les vulnérabilités logicielles (logiciels malveillants, virus et autres). Leur accès est régi par des codes utilisateurs et des mots de passe personnels.

Les actifs informationnels, propriété du Collège, peuvent être modifiés, remplacés, déplacés et retirés par le STI selon les besoins de l'établissement et à la suite d'un préavis raisonnable. Leur attribution et la gestion des droits de configuration des équipements du Collège sont également la responsabilité exclusive du STI, qui peut interdire l'accès au réseau du Collège à tout poste de travail ou équipement qu'il juge non conforme.

Aucune copie de sécurité des disques locaux n'étant effectuée, le Collège n'est pas responsable de la perte de ces données.

6.2.4 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 usager obtient un compte unique qui l'identifie. Les usagers ne doivent pas entraver le fonctionnement des outils de sécurité tels que l'antivirus, les sauvegardes de données, les dispositifs de verrouillage et les outils de contrôle d'accès.

6.2.5 Déplacement et disposition des équipements

Seuls les personnes autorisées par le STI, peuvent déplacer, installer et autoriser la disposition des équipements informatiques, téléphoniques, réseautiques et de multimédias fixes.

Le déplacement d'équipements hors des locaux du Collège doit être autorisé par le STI. L'usager est responsable d'assurer la sécurité et la protection de ces équipements.

6.2.6 Prise de copie de sécurité

Toute information hébergée sur un serveur du Collège fait l'objet d'une sauvegarde de sécurité périodique;

- 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 en vigueur au Collège.

6.2.7 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 Collège établit les règles suivantes quant à l'utilisation de ses systèmes de courriel.

Pour tout message électronique transmis à partir du réseau du Collège, l'usager 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 destinés;
- Faire preuve de vigilance en évitant d'ouvrir un courrier électronique de provenance inconnue ou douteuse.

6.3 Absence et départ d'un usager

Lors du départ temporaire ou définitif d'un usager, le STI modifie les droits d'accès et les privilèges en vigueur conformément à la directive sur la gestion des comptes usagers.

6.4 Destruction des fichiers d'une personne n'étant plus un usager

À moins de circonstances exceptionnelles, au plus tard dix (10) jours suivant la fin du lien d'adhésion ou d'emploi avec le Collège, le STI prend en charge les comptes et les répertoires de la personne qui n'est plus usager. Il en assume la gestion en collaboration avec le supérieur immédiat et en appliquant la directive sur la gestion des comptes usagers.

Le STI s'assure que la directive sur la gestion des comptes usagers est connue par les personnes concernées. Toute destruction de fichiers reliés aux comptes d'un ancien usager est effectuée sans préavis et à l'échéance du délai prévu. Le Collège ne peut être tenu responsable de la destruction de ces fichiers.

Par contre, le Collège offre aux personnes retraitées de conserver leur adresse de courriel. Le cas échéant, ces derniers peuvent l'utiliser dans le respect de la présente politique.

6.5 Intervention dans le compte d'un usager

Toute intervention dans le compte d'un usager doit être justifiée en conformité avec la directive sur la gestion des comptes usagers.

6.6 Vérification de l'utilisation

Si la direction du Collège a des motifs raisonnables de croire qu'un usager commet une infraction à la présente politique ou à une loi, il pourra procéder, en conformité avec les modalités d'intervention prévues à la directive sur la gestion des comptes usagers. Ce droit de vérification sera exercé avec circonspection et sera limité à ce qui est nécessaire pour vérifier l'infraction suspectée.

6.7 Entente de confidentialité – entreprise et organisme

Avant d'entreprendre une relation d'affaires avec le Collège, les représentantes ou représentants autorisés de toute entreprise ou de tout organisme s'engagent à respecter la présente politique et à signer le document « Entente de confidentialité » confirmant leur compréhension et leur acceptation des conditions énoncées dans ledit document.

Article 7 – GESTION DES RISQUES

L'analyse de risques guide l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre lors de leur déploiement dans l'environnement du Collège. La gestion des risques liés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Collège. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Par ailleurs, une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaitre la valeur de l'information à protéger. Ce type de catégorisation est effectué par le responsable de la sécurité de l'information (RSI), dont la fonction est définie à l'article 11.4 de la présente politique, en collaboration avec les différents propriétaires de l'information. Elle permet d'identifier le niveau de risque des actifs, leur seuil de criticité ainsi que l'impact de leur éventuelle non-disponibilité. En outre, elle permet d'identifier clairement les actions à poser en priorité lors d'un incident majeur.

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 auxquelles elle est exposée;
- Des conséquences de la réalisation de ces risques;
- Du niveau de risque acceptable pour le Collège.

7.1 Protection physique des actifs informationnels

Conformément aux pratiques dans le domaine des TI, le Collège met en place et entretient des moyens de sécurité et de contrôle afin d'empêcher tout dommage ou toute utilisation non autorisée des actifs informationnels.

7.2 Confidentialité, sauvegarde et intégrité des données

L'utilisation des actifs informationnels doit se faire de manière à protéger la confidentialité et l'intégrité des données qu'ils contiennent.

7.2.1 Responsabilité des usagers

L'usager qui utilise les actifs informationnels est responsable de la précision, de l'intégrité, de la sécurité de l'information et des traitements effectués sur les données auxquelles il a accès et qu'il utilise dans le cadre de son travail ou de ses études. Il doit :

- Protéger l'accès, l'intégrité et la confidentialité des renseignements personnels auxquels il a accès, et ce, en vertu de la *Loi sur l'accès aux documents publics des organismes publics et sur la protection des renseignements personnels*;
- Sauvegarder régulièrement ses données afin de pouvoir les récupérer à la suite d'un incident;
- En matière de courrier électronique, respecter, lorsqu'il y a lieu, la confidentialité et l'intégrité des messages transportés sur le réseau;
- En matière de gestion documentaire, s'assurer de détruire de manière sécuritaire tous les documents contenant des informations personnelles ou confidentielles en utilisant les contenants prévus à cet effet par le Collège.

7.2.2 Compte associé à des organismes, syndicats et partenaires externes

Les données des boîtes courriel et des répertoires associés à des organismes, syndicats et partenaires externes sont leur propriété. Il est donc recommandé que ces derniers effectuent une copie de sauvegarde de ces données.

7.3 Détection de contenus illégaux

Si, à l'occasion de ses opérations courantes, incluant la journalisation, le STI détecte des contenus illégaux ou contrevenant aux dispositions de la présente politique, le supérieur immédiat (dans le cas d'un membre du personnel) ou le cadre responsable (dans le cas d'un étudiant) en est saisi et l'usager peut être sanctionné.

7.4 Conservation, rétention et destruction des données

Toute donnée contenue dans les actifs informationnels est conservée, détruite ou mise au rebut de façon sécuritaire et en respectant les règles de conservation prévues au calendrier de conservation du Collège.

7.5 Plan de continuité et de relève informatique

Un plan de continuité et de relève informatique des actifs informationnels du Collège est mis en place par le STI et fait l'objet de tests et de simulations périodiques. Pour des raisons de sécurité, ce plan demeure confidentiel.

Article 8 – GESTION DES INCIDENTS

Le Collège déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires afin de :

- Limiter l'occurrence des incidents en matière de sécurité de l'information;
- Gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Un processus de gestion des incidents pour le Collège est mis en place par le STI, incluant la gestion des incidents majeurs, dont les incidents de sécurité.

Dans la gestion des incidents, le Collège peut exercer ses pouvoirs et ses prérogatives eu égard à toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

8.1 Maintenance des applications et des processus d'exploitation

L'environnement servant à effectuer la maintenance des applications et des processus doit être, dans le meilleur des cas, 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 Collège ne doivent être accessibles que par l'intermédiaire de moyens sécurisés dans un environnement contrôlé et restreint.

Toute opération critique effectuée sur une application ou 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 Collège 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.

8.2 Signalement des incidents

Il est de la responsabilité de tous les usagers de signaler au STI, 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.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale.*

Article 9 – DROIT D'AUTEUR ET PROPRIÉTÉ INTELLECTUELLE

Le Collège a le souci du respect des droits et des obligations associées à l'acquisition et à l'utilisation des logiciels et des informations présentes sur ses réseaux qui sont protégés par le droit d'auteur ou par des ententes en vigueur.

Les usagers doivent se conformer aux exigences de la *Loi sur le droit d'auteur du Canada* et les ententes intervenues entre le Collège 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.

C'est pourquoi :

- Les reproductions de logiciels ou d'objets numérisés protégés par le droit d'auteur ne sont autorisées qu'à des fins de copies de sécurité ou selon les conditions de la licence d'utilisation qui les régit;
- Tout usager doit s'abstenir d'effectuer ou de participer à la reproduction, à la diffusion de logiciels, de vidéos, de photos, d'objets numérisés ou de leur documentation à d'autres fins que celles décrites dans les conventions de droit d'auteur. Il ne peut modifier ou détruire ces fichiers sans l'autorisation de son propriétaire ou du Collège;
- Tout usager doit s'abstenir d'utiliser et de diffuser des reproductions illicites de logiciels, de progiciels, de vidéos, de photos ou d'objets numérisés sur les équipements informatiques ou sur les réseaux de télécommunications appartenant au Collège ou sur tout autre équipement informatique ou de télécommunication ne lui appartenant pas, mais utilisé dans ses locaux;
- Tout usager doit faire une demande au STI pour toute acquisition de logiciels qu'il désire utiliser au Collège, dans le cadre de ses fonctions ou de ses travaux même si celui-ci est gratuit.

Article 10 – SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté du Collège doivent être sensibilisés :

- À la sécurité de l'information et des systèmes d'information du Collège;
- 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 rendus disponibles sur le portail interne du Collège.

Article 11 – RÔLES ET RESPONSABILITÉS

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

La direction est responsable d'assurer la gestion des actifs informationnels du Collège. Elle a aussi la responsabilité de s'assurer qu'un soutien aux usagers est fourni.

Cependant, le Collège n'assume aucune responsabilité, directe ou indirecte, pour toute perte, tout dommage ou tout inconvénient causés à un usager à l'occasion ou en conséquence de l'utilisation des actifs informationnels, ou advenant le cas où elle devrait, pour quelque cause que ce soit, diminuer ses services, ou les interrompre, quelle que soit la durée d'une telle diminution ou interruption, ou encore arrêter définitivement ses services.

11.1 Conseil d'administration

Le conseil d'administration adopte la Politique de sécurité de l'information et de protection des renseignements personnels ainsi que toute modification à celle-ci. Le conseil est tenu informé des actions du Collège en lien avec la présente politique.

11.2 Direction générale

La Direction générale veille à l'application de la politique sur la sécurité de l'information et :

- Encadre le responsable de la sécurité de l'information (RSI) dans la réalisation de son mandat;
- Tient informé le CA des orientations stratégiques, évaluations de risques, plans d'action, bilans de sécurité et redditions de comptes en matière de sécurité de l'information;
- Autorise, de façon exceptionnelle, une dérogation à l'une ou l'autre des dispositions de la présente politique, 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 Collège.

11.3 Comité de gestion

Le comité de gestion collabore à la conception des plans d'action et des bilans de sécurité de l'information issus des travaux du Comité de travail sur la sécurité de l'information. Il peut également proposer des directives et des procédures qui viennent préciser ou soutenir l'application de la politique.

11.4 Responsable de la sécurité de l'information (RSI)

La fonction de RSI est déléguée à un membre du personnel cadre par le conseil d'administration. Le RSI relève directement de la direction générale au sens du Cadre gouvernemental de gestion de la sécurité de l'information. Cette personne met en place le cadre de gestion de la sécurité de l'information et s'assure que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins.

Le RSI :

- Élabore et propose le programme de sécurité de l'information du Collège et rend compte de son implantation à la direction générale;
- Formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et met à jour la politique;
- Assure la coordination et la cohérence des actions menées au sein de la communauté collégiale en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans les unités;
- Produit les plans d'action, les bilans et les redditions de comptes du Collège en matière de sécurité de l'information;
- Propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;
- S'assure de la déclaration par le Collège des risques et des incidents de sécurité de l'information à portée gouvernementale (CERT/AQ);
- Collabore à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille à leur déploiement;
- Procède aux enquêtes relatives aux transgressions sérieuses, présumées ou avérées, à l'égard de la présente politique selon les procédures d'enquêtes prévues;
- S'assure des veilles normative, juridique, gouvernementale et technologique afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

11.5 Comité de travail pour la sécurité de l'information

Le comité de travail pour la sécurité de l'information conçoit le cadre de gestion de la sécurité de l'information pour assurer la protection du Collège et être conforme à la réglementation.

Ce comité est chargé en particulier d'élaborer les plans d'action et les bilans de sécurité de l'information, les activités de sensibilisation ou de formation ainsi que toutes propositions d'action en matière de sécurité de l'information. C'est aussi un forum d'échange sur la sécurité de l'information et son évolution.

Le comité est formé du responsable de la sécurité de l'information, qui en assume la responsabilité, du coordonnateur du Service des technologies de l'information, du directeur ou de la directrice des affaires corporatives, du développement institutionnel et des communications, d'un cadre de l'organisation scolaire, d'un technicien ou d'une technicienne informatique désigné(e) par la coordination du STI et d'une personne issue de chacune des catégories de personnel. Le comité pourra s'adjoindre d'autres représentants ou représentantes des usagers au besoin.

11.6 Service des technologies de l'information (STI)

Le STI prend en charge ce qu'exige la 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 il intervient.

- Il 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;
- Il 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.

De façon plus précise, le STI est responsable de :

- Sauvegarder régulièrement et de protéger l'intégrité des données et des fichiers de toutes natures conservés dans les serveurs gérés par le Collège, qu'il en soit propriétaire ou non;
- Récupérer les données à la suite d'un incident;
- Protéger les usagers contre les virus, les intrusions ou les altérations de données;
- Prévenir des utilisations illicites;
- S'assurer de la confidentialité des données et des fichiers de chacun des comptes d'usagers qu'il gère sous réserve de l'article 6.4;
- Gérer les accès et la journalisation des événements qui surviennent sur les réseaux et les systèmes;
- Gérer les comptes usagers, leurs accès, leur protection, ainsi que l'accès aux réseaux;
- Installer, mettre en place, entretenir, réparer, modifier et retirer les actifs informationnels;
- Acquérir les systèmes d'informations et le respect des clauses contractuelles les concernant (ententes sur l'utilisation, respect du droit d'auteur, licences, ententes sur des bases de données, etc.);
- Reproduire des logiciels ou d'objets numérisés protégés dans le respect du droit d'auteur ou conformément aux licences ou aux ententes;
- Détruire, des fichiers illégaux ou à caractère illicite, enregistrés sur les serveurs du Collège conformément à la procédure établie;
- Vérifier, sur demande d'une personne autorisée, l'information entreposée ou transitant sur les réseaux du Collège;
- Rendre disponible à toute personne autorisée les équipements, des logiciels et des applications disponibles au STI et le soutien nécessaire à leur utilisation dans le cadre de la mission du Collège;
- Fournir un soutien adéquat aux usagers utilisant les technologies de l'information et des communications.

11.7 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 Collège 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 responsable de la sécurité de l'information (RSI) en vue de déterminer, de gérer, de coordonner et de mettre en œuvre des mesures de sécurité de l'information, indépendamment de son support.

À titre de responsable de l'accès à l'information et de la protection des renseignements personnels, la DACDIC :

- Veille au respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);
- Communique au responsable de la sécurité de l'information (RSI) les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles;
- Contribue à assurer la cohérence des interventions relatives à la sécurité de l'information, à l'accès aux documents et à la protection des renseignements personnels, y compris lors de la mise en œuvre du processus de gestion des risques et des incidents de sécurité de l'information.

11.8 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 Collège.

11.9 Service des ressources humaines

Le service des ressources humaines obtient de tout nouveau membre du personnel du Collège son engagement au respect de la présente politique, après lui en avoir expliqué la nécessité.

11.10 Responsable d'actifs informationnels

Le ou la responsable d'actifs informationnels est un cadre dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de son service, que l'actif soit d'ordre pédagogique ou administratif. Il peut donc y avoir plusieurs responsables d'actifs informationnels au Collège et leur responsabilité est précisée dans l'annexe sur la catégorisation des actifs. Le ou la responsable d'actifs informationnels peut déléguer une partie de sa responsabilité à un autre membre du service.

Le ou la responsable d'actifs informationnels :

- Informe le personnel relevant de son autorité, et les tiers avec lesquels il ou elle transige, de la politique de sécurité de l'information et de protection des renseignements personnels et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer;
- Collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques;
- Voit 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 relevant de son autorité en conformité avec la présente politique et de tout autre élément du cadre de gestion;
- S'assure que les exigences en matière de sécurité de l'information et de protection des renseignements personnels sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du cadre de gestion;
- Rapporte au Service des technologies de l'information toute menace ou tout incident relatifs à la sécurité de l'information;
- Collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information et la protection des renseignements personnels ou à remédier à un incident de sécurité ainsi qu'à toute opération de vérification de la sécurité de l'information;
- Rapporte à l'autorité responsable tout problème lié à l'application de la présente politique, dont toute contravention réelle ou apparente à cette politique.

11.11 Usagers

La responsabilité de la sécurité de l'information du Collège incombe à tous les usagers des actifs informationnels, sauf dans le cas d'une usurpation d'identité.

Tout usager qui accède à une information, qui la consulte ou qui la traite est responsable de l'utilisation qu'il en fait et doit procéder de manière à protéger cette information.

Chaque usager doit :

- Se conformer à la présente politique et à toute autre directive du Collège en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- 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;
- Participer, au besoins, à la catégorisation de l'information de son service;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
- Signaler au responsable des actifs informationnels de son unité tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l'information du Collège;
- Collaborer à toute intervention visant à contrer une menace à la sécurité de l'information ou un incident de sécurité de l'information;
- Informer le STI de tout usage non autorisé de ses codes d'accès et mots de passe.

Un usager doit acheminer au STI toute demande relative à la mise en place, à l'installation, à la réparation et au retrait des actifs informationnels et toute demande d'acquisition d'actifs informationnels préalablement autorisées.

Aussi, tout usager doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles ou d'études, lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

Article 12 – SANCTIONS

En plus des pénalités prévues à la Loi, tout usager qui contrevient à la présente politique est passible des sanctions suivantes :

- Suspension ou annulation de ses privilèges d'accès aux actifs informationnels du Collège;
- Destruction sans préavis des fichiers constitués contrairement à la présente politique, illégalement ou comportant des renseignements à caractère illicite;
- Remboursement au Collège de toute somme que ce dernier serait dans l'obligation de payer, y compris toute réclamation, tous frais de justice ou dommages à la suite du non-respect de la présente politique;
- Mesures disciplinaires ou sanctions pouvant aller jusqu'au congédiement ou à l'expulsion conformément aux règlements ou aux protocoles en vigueur au Collège et dans le respect des dispositions des conventions collectives.

Article 13 – DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le Responsable de la sécurité de l'information s'assure de la diffusion et de la mise à jour de la politique. La politique de sécurité de l'information est révisée au besoin.

Article 14 – ENTRÉE EN VIGUEUR

La présente politique abroge et remplace la *Politique concernant l'utilisation des ressources informatiques, des communications et de l'Internet (RICI) SA-12-PO-01*, dont le contenu a été intégré à la présente politique, et entre en vigueur dès son adoption par le conseil d'administration.

Article 15 – RÉFÉRENCES ET SOURCES

15.1 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)*

15.2 Références

Cette Politique de sécurité de l'information et de protection des renseignements personnels 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.*
- *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.*
- *Gabarit de Politique de sécurité de l'information de la Fédération des cégeps, Mars 2017*

ANNEXE A

EXTRAITS ET RÉFÉRENCES À DES TEXTES LÉGAUX EN RELATION AVEC LA POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

A. CHARTE DES DROITS ET LIBERTÉS DE LA PERSONNE (L.R.Q., c. C-12)

- Art. 1 : Tout être humain a droit à la vie privée, ainsi qu'à la sûreté, à l'intégrité et à la liberté de sa personne.
- Art. 4 : Toute personne a droit à la sauvegarde de sa dignité, de son honneur, de sa réputation.
- Art. 5 : Toute personne a droit au respect de sa vie privée.
- Art. 10 : Toute personne n'a droit à la reconnaissance et à l'exercice, en pleine égalité, des droits et libertés de la personne, sans distinction, exclusion ou préférence fondée sur la race, la couleur, le sexe, la grossesse, l'orientation sexuelle, l'état civil, l'âge sauf dans la mesure prévue par la loi, la religion, les convictions politiques, la langue, l'origine ethnique ou nationale, la condition sociale, le handicap ou l'utilisation d'un moyen pour pallier ce handicap.
- Art. 10.1 : Nul ne doit harceler une personne en raison de l'un des motifs visés dans l'article 10.

B. CODE CIVIL DU QUÉBEC (L.Q. 1991, C.64)

- Art. 3 : Toute personne est titulaire de droits de la personnalité, tel le droit à la vie, à l'inviolabilité de son nom, de sa réputation et de sa vie privée.
- Art. 35 : Toute personne a droit au respect de sa vie privée. Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci ou ses héritiers y consentent ou sans que la loi l'autorise.
- Art. 36 : Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants :
    a) Pénétrer chez elle ou y prendre quoi que ce soit;
    b) Intercepter ou utiliser volontairement une communication privée;
    c) Capter ou utiliser son image ou sa voix lorsqu'elle se trouve sur des lieux privés;
    d) Surveiller sa vie privée par quelque moyen que ce soit;
    e) Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;
    f) Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

Voir aussi : Art. 1379, 1435, 1457, 1465.

C. CODE CRIMINEL (C-46)

- Art. 183 : (Communication privée) Toute communication orale ou télécommunication faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par une personne autre que celle à laquelle il la destine.
- Art. 184 : Quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée est coupable d'un acte criminel à moins d'avoir obtenu le consentement préalable de l'auteur de la communication privée ou de la personne à laquelle son auteur la destine.

- Art. 342.1C.cr.: Quiconque, « fondamentalement et sans apparence de droit », obtient les services d'un ordinateur, intercepte une fonction d'un ordinateur, utilise un ordinateur pour ses fins ou pour commettre un méfait, est passible d'une peine maximale de 10 ans d'emprisonnement.
- Art. 430 (1.1) : Quiconque volontairement :
  a) « détruit ou modifie des données;
  b) dépouille des données de leur sens, les rend inutiles ou inopérantes;
  c) empêche, interrompt ou gêne l'emploi légitime des données;
  d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit » est passible d'une peine maximale de dix ans d'emprisonnement. (L'introduction d'un virus informatique serait un exemple d'un tel délit)

Voir aussi : Art. 361.

D. LOI SUR DROIT D'AUTEUR (C-42)

- Art. 2 : (Définition de « programme d'ordinateur ») Ensemble d'instructions ou d'énoncés destiné, quelle que soit la façon dont ils sont exprimés, fixés, incorporés ou emmagasinés, à être utilisé directement ou indirectement dans un ordinateur en vue d'un résultat particulier.
- Art. 3. (1) : (Définition de « droit d'auteur ») pour l'application de la présente loi, « droit d'auteur » s'entend du droit exclusif de produire ou de reproduire une œuvre, ou une partie importante de celle-ci, sous une forme matérielle quelconque.... Ce droit s'entend, en outre, du droit exclusif :
  a) de produire, reproduire, représenter ou publier une traduction de l'œuvre;
  b) de louer un programme d'ordinateur qui peut être reproduit dans le cadre normal de son utilisation, sauf la reproduction effectuée pendant son exécution avec un ordinateur ou autre machine ou appareil.
- Art. 13. (1) : Sous réserve des autres dispositions de la présente loi, l'auteur d'une œuvre est le premier titulaire du droit d'auteur sur cette œuvre.
- Art. 14.1 (1) : L'auteur d'une œuvre a le droit, sous réserve de l'article 28.2, à l'intégrité de l'œuvre et à l'égard de tout acte mentionné à l'article 3, le droit, compte tenu des usages raisonnables, d'en revendiquer, même sous pseudonyme, la création, ainsi que le droit à l'anonymat.
- Art. 14.2 (1) : Les droits moraux sur une œuvre ont la même durée que le droit d'auteur sur celle-ci.
- Art. 27 (1) : Est considéré comme ayant porté atteinte au droit d'auteur sur une œuvre quiconque, sans le consentement du titulaire de ce droit, exécute un acte qu'en vertu de la présente Loi seul ce titulaire a le droit d'exécuter.

E. LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS (L.R.Q., c. A-2.1)

Particulièrement les articles 53 à 102.1