CÉGEP RÉGIONAL *de* LANAUDIÈRE

TITRE : **Politique sur la sécurité de l'actif informationnel**

Adoption par le conseil d'administration :

Résolution : **CARL-130924-11**
Date : **24 septembre 2013**

Révision :

Résolution : **CARL-191126-17**
Date : **26 novembre 2019**

TABLE DES MATIÈRES

PRÉAMBULE

La *Politique sur la sécurité de l'actif informationnel* (ci-après la « Politique ») vise la protection de l'information créée ou reçue sous la responsabilité du Cégep régional de Lanaudière (CRL). Cette information multiple et diversifiée consiste en des renseignements personnels d'étudiants et de membres du personnel, en de l'information professionnelle sujette à des droits de propriétés intellectuelles et, finalement, en de l'information stratégique ou opérationnelle pour l'administration du CRL.

1. CHAMP D'APPLICATION

La présente Politique s'adresse à tout le personnel, à toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public utilise les actifs informationnels du CRL.

L'information visée est celle que le CRL détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers. Tous les supports de données, électroniques ou autres sont concernés.

2. OBJECTIFS

La présente Politique a pour objectif d'affirmer l'engagement du CRL à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, le CRL 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 CRL met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information de l'institution.

Le cadre de gestion de la sécurité de l'information renforce 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 CRL en matière de réduction du risque associé à la protection de l'information.

3. DÉFINITIONS

« Actif informationnel » : les documents, les systèmes, les bases de données et les équipements permettant le traitement, le transport et l'entreposage d'information. On y retrouve notamment les systèmes de téléphonie et de vidéoconférence, l'infrastructure sans-fil, serveurs de courriels, les renseignements enregistrés dans les systèmes de stockage informatique, de même que les réseaux informatiques mis à la disposition des utilisateurs.

« Équipement informatique » : les composantes et les équipements réseau, les serveurs informatiques, les postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information; tout équipement de télécommunications; les logiciels, les progiciels, les didacticiels, les documents ou les banques de données et de renseignements installés sur un média informatique; le système de courrier électronique, le système de messagerie vocale ou toute autre infrastructure mise en place par le CRL.

« Confidentialité » : propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées.

« Disponibilité » : propriété d'une information d'être accessible en temps voulu et de la manière requise pour une personne autorisée.

« Intégrité » : propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

« Cycle de vie de l'information » : l'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation défini par le CRL.

« Utilisateur » : tous les membres du personnel du Cégep, les étudiants et toute personne physique ou morale autorisée à avoir accès à l'environnement informatique.

4. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du CRL en matière de sécurité de l'information sont les suivants :

- *Protection de l'information*

Le CRL met en place des mesures de protection, de prévention, de détection et de correction tout au long du cycle de vie de l'actif informationnel, qui permettent d'assurer la confidentialité, l'intégrité, la disponibilité, l'authentification et l'irrévocabilité de même que la continuité des activités. Ces mesures préviennent notamment les accidents, l'erreur, la malveillance, l'indiscrétion ou la destruction d'information sans autorisation.

- *Protection des renseignements personnels*

  Protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle afin de s'assurer que ceux-ci sont utilisés et ne servent qu'aux fins pour lesquelles ils ont été recueillis ou obtenus.

- *Propriété des données*

  Sauf pour les informations assujetties à la Loi sur le droit d'auteur et les documents produits par les enseignants et les étudiants dans le cadre d'activités pédagogiques, toute information de nature administrative – y compris en lien avec le cheminement scolaire des étudiants – est la propriété unique du cégep, qu'elle soit sauvegardée dans les infrastructures informatiques du cégep ou encore hébergée à l'extérieur par un fournisseur en vertu d'une entente avec ce dernier.

- *Utilisation adéquate des outils*

  Le cégep met à la disposition des utilisateurs des équipements informatiques et d'échange d'information qui doivent être utilisés à des fins professionnelles ; il prend les moyens appropriés pour s'assurer d'une juste utilisation des éléments de l'actif informationnel.

- *Pratiques reconnues*

  Les actions du CRL prennent appui sur des normes internationales pertinentes en matière de gestion des technologies de l'information, au regard notamment de la disponibilité et de la confidentialité dans l'utilisation des technologies de l'information et ce pour favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou des établissements similaires.

- *Sensibilisation et formation*

Le CRL s'engage, sur une base régulière, à sensibiliser et à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

5. CADRE DE GESTION

La mise en œuvre de la présente Politique s'appuie sur la définition d'un cadre de gestion en sécurité de l'information qui précise le champ d'action des différents intervenants. Le cadre de gestion précise l'organisation fonctionnelle en matière de sécurité de l'information et rend possible la définition d'objectifs clairs et une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information sont réévaluées de manière périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces et des risques.

La Politique de sécurité de l'information du CRL s'articule ainsi autour de trois axes fondamentaux de gestion. Ces axes sont la gestion des accès, la gestion des risques et la gestion des incidents.

5.1 Gestion des accès

La gestion des accès est encadrée et contrôlée pour faire en sorte que l'accès, la divulgation et l'utilisation de toute information détenue par le CRL soient strictement réservés aux personnes autorisées.

5.2 Gestion des risques

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

5.3 Gestion des incidents

La gestion des incidents se caractérise par la mise en place de procédures de compte rendu, d'analyse relativement aux incidents de sécurité et de mesures correctives pour y donner suite. Les mesures déployées visent à assurer la continuité des services.

Dans la gestion des incidents, le CRL peut exercer ses pouvoirs et ses prérogatives en lien avec toute utilisation inappropriée de l'information qu'il détient ou des systèmes d'information qu'il gère.

6 RÔLES ET RESPONSABILITÉS

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

6.1 Direction générale

La direction générale fait adopter par le conseil d'administration les orientations stratégiques, les évaluations de risques, les plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information.

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

La fonction du RSI est déléguée à un cadre par le conseil d'administration. Le RSI relève 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. Il est nommé par le conseil d'administration.

6.3 Direction des ressources matérielles et des technologies de l'information

La direction des ressources matérielles et des technologies de l'information assume la responsabilité de l'application de la présente Politique. Elle s'assure de la prise en charge des exigences de 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.

De plus, elle 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 CRL.

6.4 Direction des ressources humaines

En matière de sécurité de l'information, la direction des ressources humaines obtient de tout nouvel employé du CRL, après lui en avoir montré la nécessité, son engagement au respect de la Politique.

6.5 Responsable d'actifs informationnels

Le responsable d'actifs informationnels est le cadre 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.

6.6 Utilisateurs

La responsabilité de la sécurité de l'information du CRL incombe à tous les utilisateurs des actifs informationnels du CRL.

Tout utilisateur 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.

À cette fin, l'utilisateur doit :

a) Se conformer à la présente politique et à toute autre directive du CRL en matière de sécurité de l'information et d'utilisation des actifs informationnels;
b) Être responsable des actions résultant de l'usage de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers, à moins qu'il démontre que les actions posées par un tiers ne découlent pas d'une négligence ou d'une malveillance de sa part;
c) Aviser une personne responsable, un enseignant ou son supérieur immédiat, de toute situation susceptible de compromettre la sécurité de l'actif informationnel;
d) Participer à la catégorisation de l'information de son service;
e) Utiliser les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre approprié à son utilisation et aux fins auxquelles ils sont destinés;
f) Respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ni les désactiver;
g) Collaborer à toute intervention visant à indiquer ou à mitiger une menace à la sécurité de l'information ou un incident de sécurité de l'information.

7 FORMATION, SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur l'adoption de comportements sécuritaires et la responsabilisation individuelle. À cet égard, les membres de la communauté du CRL doivent être sensibilisés :

- À la sécurité de l'information et des systèmes d'information du CRL ;
- Aux conséquences d'une atteinte à la sécurité ;
- À leur rôle et à leurs responsabilités en la matière.

8 SANCTIONS

En cas de contravention à la présente Politique, l'utilisateur engage sa responsabilité personnelle; il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

Tout membre de la communauté collégiale qui contrevient au cadre légal, à la présente Politique et aux mesures de sécurité de l'information qui en découlent, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles administratives ou disciplinaires internes applicables.

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

9 RESPONSABLE DE LA POLITIQUE

Le RSI est responsable de la diffusion et de la mise en application de la Politique

10 ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur à la date de son adoption par le conseil d'administration.