CÉGEP RÉGIONAL *de* LANAUDIÈRE

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

Adoption par le conseil d'administration :

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

Révisions :

Résolution :
Date :

Table des matières

1. Préambule

L'environnement informatique a pris une place de plus en plus importante au sein de notre organisation. À bien des égards, on ne peut plus s'imaginer sans un environnement informatique qui permet une connectivité à des réseaux, le versement et la sauvegarde de données, le traitement de celles-ci dans des systèmes de gestion et l'accès à un parc de postes informatiques.

Ce document vise à préciser les principes généraux et les responsabilités inhérentes à une saine gestion des technologies de l'information dans le but d'offrir aux usagers et au cégep un environnement technologique sécuritaire. Ce dernier comprend à la fois les services offerts à l'intérieur des murs du cégep tout comme les services disponibles pour le cégep en mode infonuagique.

Le Cégep reconnaît que la sécurité concernant les technologies de l'information est vitale à son bon fonctionnement. La sécurité de ses systèmes et des infrastructures est pertinente pour tous les domaines d'activités du cégep. Il importe de protéger l'actif informationnel afin que les activités pédagogiques et administratives ne soient pas compromises.

Cette politique s'additionne aux dispositions du Règlement sur l'informatique et la téléinformatique et les directives en découlant. Cette politique guide chaque individu de notre communauté collégiale afin qu'il soit conscient de sa propre responsabilité à l'égard de la sécurité informatique et qu'il fasse preuve d'un comportement responsable.

2. Définitions

Disponibilité :	l'aptitude d'un système à assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la requête de service en est faite.
Intégrité :	la protection de l'exactitude et de l'entièreté de l'information et des méthodes de traitement de celle-ci.
Actif informationnel :	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, les renseignements inscrits sur support informatique, de même que les réseaux électroniques mis à la disposition des usagers.

Équipement informatique :	les composantes et les équipements réseaux, 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 télécommunication; les logiciels, les progiciels, les didacticiels, les documents ou les banques de données et de renseignements placées dans un équipement ou sur un média informatique; le système de courrier électronique et le système de messagerie vocale.
Employé :	une personne à l'emploi du Cégep régional de Lanaudière.
Étudiant :	une personne admise au cégep dans un programme d'études collégiales et inscrite à un ou à des cours de ce programme, au collège ou en commandite.
Gestionnaire de système :	le gestionnaire responsable des aspects opérationnels d'un système corporatif (ressources humaines, ressources financières, cheminement scolaire, impression, etc.) ou d'une plateforme d'enseignement (Moodle, etc.)
Usager :	tous les membres du personnel du Cégep, les étudiants et toute personne physique ou morale autorisée à avoir accès aux équipements informatiques.
Utilisateur :	tous les membres du personnel du Cégep et toute personne physique ou morale autorisée à avoir accès à un système de gestion;

3. But de la politique

La présente politique vise à préciser les principes généraux et les responsabilités inhérentes à une saine gestion des technologies de l'information dans le but d'offrir aux usagers et au cégep un environnement technologique sécuritaire.

4. Destinataires

La présente politique s'applique à toute personne physique ou morale qui utilise ou accède à l'actif informationnel du cégep. Les personnes morales peuvent être, notamment, mais non limitativement, les fournisseurs de service ou de biens mandatés par le cégep devant accéder au réseau, à des applications du cégep, au parc informatique ou encore devant intervenir ou supporter les systèmes de gestion.

5. Responsable de l'application

La Direction des ressources informationnelles du Cégep régional de Lanaudière est responsable de l'application de la Politique.

6. Objectifs

La présente politique et les mesures qui en découlent visent à :

- Protéger l'actif informationnel du cégep afin de permettre la tenue de toutes les activités prévues, dans les meilleures conditions.
- Appliquer les bonnes pratiques de sécurité et documenter celles-ci afin de mieux gérer la protection de l'actif informationnel.
- Définir les attentes au regard du comportement des usagers afin que ceux-ci contribuent également à la gestion sécuritaire des ressources informationnelles.

7. Principes généraux

a) 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.

b) Utilisation adéquate des outils

Le Cégep met à la disposition des usagers des équipements informatiques et d'échange d'information qui doivent être utilisés à des fins professionnelles. Conformément au Règlement sur l'informatique et la téléinformatique, le Cégep prend les moyens appropriés pour s'assurer d'une juste utilisation des éléments de l'actif informationnel par les usagers.

c) Mesures de protection

Le Cégep met en place des mesures de protection, de prévention, de détection et de correction qui permettent d'assurer la confidentialité, l'intégrité, la disponibilité, l'authentification et l'irrévocabilité de l'actif informationnel 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.

d) Protection des renseignements personnels

Les renseignements personnels sont utilisés et ne servent qu'aux fins pour lesquelles ils ont été recueillis ou obtenus. La collection, la transmission, l'échange ou la communication de données nominatives se réalisent dans le respect des lois en cette matière et des exigences découlant de directives, des règles et des procédures mises de l'avant par le Cégep.

e) Application de normes reconnues

Le Cégep applique des normes reconnues 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. Ces normes nécessitent des actions appropriées des usagers.

8. Niveaux de risques et sécurité

Afin de remplir son mandat comme prestataire de services, la Direction des ressources informationnelles détermine les niveaux de risques acceptables et évalue les menaces touchant l'actif informationnel. Elle établit des directives adéquates reliées à l'exécution des opérations informatiques et à leurs résultats. Elle s'assure, en collaboration avec les autres gestionnaires, que tous les usagers utilisent de façon sécuritaire l'actif informationnel.

9. Accès aux systèmes de gestion

Les systèmes de gestion pédagogiques ou administratifs sont des éléments de l'actif informationnel pouvant représenter un niveau élevé de risques. Chaque système de gestion prévoit des mécanismes permettant d'accorder des droits d'accès différents selon les catégories d'utilisateurs et de vérifier toutes les actions posées sur les données sensibles.

Le droit d'accès d'un utilisateur aux systèmes de gestion est attribué en fonction de ce qui est nécessaire pour l'exécution des tâches qu'il a à accomplir. Cette règle s'applique également au personnel responsable du soutien informatique.

Le cégep documente les accès donnés à chacun des utilisateurs dans un registre. Ce registre, sous la responsabilité de la Direction des services informationnels, contient notamment, le nom des personnes, leur rôle et les droits d'intervention qui leur sont attribués. Ce registre est mis à jour régulièrement.

Pour chacun des systèmes informationnels, une procédure doit décrire la gestion des droits d'accès de ses utilisateurs. Chaque accès fait l'objet d'une autorisation formelle par une personne responsable. Les mots de passe utilisés par les utilisateurs doivent correspondre au minimum des standards de sécurité déterminés par la présente politique. Les utilisateurs doivent également adopter les pratiques et mesures généralement reconnues afin de sécuriser leur poste de travail en leur absence.

10. Accès au réseau et mot de passe

Un code d'accès individuel est alloué à un utilisateur par le Cégep à titre personnel et confidentiel. Il en est de même pour le mot de passe. L'utilisateur est responsable des communications ou des actions sur le réseau et dans des applications initiées par l'utilisation son code d'accès et de son mot de passe; de ce fait, il a la responsabilité de les protéger.

Dans une perspective de sécurité et afin de répondre aux normes actuelles en matière de sécurité, seuls les mots de passe respectant les critères suivants seront acceptés pour l'authentification sur le réseau et dans les systèmes de gestion :

- Minimum huit (8) caractères
- Inclusion d'une ou plusieurs lettres majuscules
- Inclusion d'une ou plusieurs lettres minuscules
- Inclusion d'un ou plusieurs chiffres ou d'un ou plusieurs caractères spéciaux

Le Cégep entend également exiger des modifications ponctuelles des mots de passe des usagers.

Un registre est tenu à jour pour décrire la liste des fournisseurs ou mandataires bénéficiant d'un accès à distance ou non au réseau.

Par le biais d'une procédure à cet effet, le Cégep détermine la durée des accès à un ou plusieurs services informatiques lorsqu'il y a une modification au lien d'emploi d'un employé, qu'il s'agisse d'un départ à la retraite, d'un départ pour un autre emploi ou toute autre situation.

11. Utilisation des réseaux externes

La Direction des ressources informationnelles utilise les normes en vigueur afin d'établir la connexion à des réseaux externes, dont Internet.

Un registre est tenu à jour pour décrire la liste des équipements raccordés à un réseau externe qui sont en lien avec des éléments de l'actif informationnel considérés comme critiques et sensibles. Le niveau d'importance des éléments de l'actif est déterminé selon la nature, l'étendue et le caractère confidentiel de l'information traitée. Ce registre contient notamment le nom des équipements, le coupe-feu utilisé, le nom du réseau externe, les logiciels, la fréquence des correctifs appliqués et le nom du responsable de cet équipement.

12. Mesures de sécurité de l'environnement informatique

La Direction des ressources informationnelles doit s'assurer de mettre en place des mesures pour protéger le réseau du cégep contre les menaces d'intrusion en déployant, au minimum, un pare-feu et un logiciel antivirus sur les serveurs et les postes de travail. La direction s'assure également de mettre en place des mesures pour informer et encadrer le personnel sur l'usage du courrier électronique et d'internet afin de parer à des menaces d'intrusion, notamment par le courrier malveillant.

13. Mesures de sécurité des installations informatiques

De concert avec la Direction des ressources matérielles, la Direction des ressources informationnelles doit s'assurer de la sécurité des infrastructures et du bon fonctionnement des équipements matériels destinés à supporter les infrastructures informatiques.

14. Mesures de sécurité pour les données

Les services informatiques prennent les mesures appropriées afin de s'assurer de l'intégrité des données. Ils s'assurent dans un premier temps que l'accès aux données est protégé en tout temps et seulement accessible par les usagers dûment authentifiés et pour les données pertinentes. Ils s'assurent de faire quotidiennement une copie des données sous sa responsabilité et que les fournisseurs afférents en fassent tout autant.

En outre, la Direction des ressources informationnelles s'assure de mettre en place les mesures appropriées pour effacer complètement le contenu des médias de stockage contenant des renseignements classifiés et protégés et des logiciels sous licence avant d'en disposer.

15. Procédures documentées

Les gestionnaires responsables s'appliquent à documenter les procédures en lien avec les éléments de l'actif informationnel jugés critiques.

La liste des systèmes et des personnes responsables de l'application des directives de sécurité est tenue à jour.

Un inventaire de tous les éléments de l'actif informationnel du cégep qui sont considérés comme critiques ou sensibles est tenu à jour. Cet inventaire décrit chacun des éléments de l'actif, son niveau d'importance et identifie le responsable de l'élément de l'actif.

16. Mandats confiés à un tiers

Les mandats confiés aux firmes externes en lien avec des éléments de l'actif informationnel qui sont considérés comme critiques ou sensibles sont décrits dans un registre. Ce registre contient notamment le nom de la ressource informationnelle en cause, les coordonnées de l'entreprise, la description du mandat confié et le nom du gestionnaire du système concerné.

17. Formation et sensibilisation

La Direction des ressources informationnelles doit :

a) Mettre en place un programme de sensibilisation en matière de sécurité pour informer les usagers de leurs responsabilités en matière de sécurité et pour leur faire des rappels périodiques à cet égard;

b) Informer les usagers des privilèges d'accès et des limites reliées à leurs tâches.

18. Rôles et responsabilités

a) La direction des ressources informationnelles :

- Assume la responsabilité de l'application de la présente politique;
- Accompagne les gestionnaires dans la mise en place des processus de sécurité;
- Assure, au besoin, la coordination entre les diverses directions du cégep et un fournisseur spécialiste en sécurité de l'information;
- Constitue un registre de l'ensemble des procédures découlant de la présente politique et des personnes responsables de leur application;
- Tient à jour, avec la collaboration des gestionnaires de systèmes de gestion, un registre des utilisateurs et leurs droits;
- Tient à jour un registre des équipements raccordés à un réseau externe qui sont en lien avec des éléments de l'actif informationnel considérés comme critiques ou sensibles;
- Maintient un registre des mandats confiés aux firmes externes en lien avec des éléments de l'actif informationnel qui sont considérés comme critiques ou sensibles;
- S'assure que les responsables des opérations menées appliquent de bonnes pratiques de gestion en matière de sécurité

b) Le gestionnaire d'un système de gestion :

- Applique et fait appliquer par le personnel sous sa responsabilité ou utilisateur de son système les directives de sécurité concernant l'actif informationnel dont il est responsable;
- Supervise en coordination avec le responsable de la présente politique, les activités nécessaires à la réalisation de mandats confiés à des entreprises externes;
- Applique les procédures de sécurité prévues concernant le système dont il est responsable;

- Accorde les accès à chacun des utilisateurs et vérifie les données du registre;
- Vérifie la cohérence des accès selon les statuts définis pour chacun des utilisateurs et les exigences de la présente politique et révise périodiquement – selon les consignes de la direction – le statut de ses utilisateurs à l'intérieur du système.

c) Le cadre :

- Informe ses employés de la politique, des directives et des procédures concernant la sécurité des technologies de l'information;
- S'assure que ses employés mettent en pratique les directives émises par le cégep.

d) L'usager :

- Prend connaissance, applique et respecte la présente politique et les directives qui en découlent, les normes et les procédures du cégep, les lois et les règlements relatifs à la sécurité des technologies de l'information;
- Est 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;
- Avise une personne responsable, un enseignant ou son supérieur immédiat, de toute situation susceptible de compromettre la sécurité de l'actif informationnel.

19. Analyses sur les incidents de sécurité

La direction des ressources informationnelles implante des procédures de compte rendu et d'analyse relativement aux incidents de sécurité et prend des mesures correctives pour y donner suite.

20. Sanctions

Conformément au Règlement sur l'informatique et la téléinformatique, du Règlement sur les conditions de vie et aux dispositions des conventions collectives le non-respect de la présente politique peut mener à la suspension des privilèges d'accès aux technologies de l'information du cégep et d'autres mesures administratives, disciplinaires ou juridiques.

21. Entrée en vigueur

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration.

22. Évaluation de la politique et révision

La présente politique doit être évaluée aux cinq ans et révisée le cas échéant.