Cégep de Sainte-Foy

2410, chemin Sainte-Foy, Québec, QC G1V 1T3
(418) 659-6600 www.cegep-ste-foy.qc.ca

Politique de sécurité de l'actif informationnel

FÉVRIER 2010

Adopté au conseil d'administration du Cégep de Sainte-Foy le 22 février 2010.

Table des matières

Préambule 3

Section 1 – Définitions 4

Section 2 – Champ d'application 5

Section 3 – Objectifs 5

Section 4 – Dispositions générales 5

Section 5 – Mesures de sécurité 6

Section 6 – Partage des responsabilités 8

Section 7 – Divers 9

Préambule

L'apport grandissant des outils technologiques dans le travail et la quantité de l'information qu'on y trouve ont entraîné des modifications majeures dans les caractéristiques de l'infrastructure technologique du Collège.

Ce document décrit la politique de sécurité concernant les technologies de l'information qui exploitent les différentes ressources de l'actif informationnel du Collège et présente les orientations à privilégier. Il fournit un cadre de référence pour la mise en œuvre des actions des usagers et les interventions des personnels qui les soutiennent.

Le Collège assure la sécurité des données des systèmes informationnels, de la connectivité (liens réseaux internes et externes), de la téléphonie et des équipements informatiques mis à la disposition des usagers.

La direction du Collège reconnaît que la sécurité concernant les technologies de l'information est vitale à son fonctionnement. La sécurité de ces systèmes concerne tous les domaines d'activités du Collège. Il importe de protéger l'actif informationnel afin que les activités ne soient pas compromises.

•

Cette politique complète les différentes lois et règlements qui encadrent les responsabilités du Collège, notamment en ce qui concerne : la protection des données opérationnelles confidentielles et les renseignements sur les individus (données personnelles et nominatives), la propriété intellectuelle et les droits d'auteur. Elle guide chaque individu afin qu'il fasse preuve d'un comportement responsable.

La présente politique de sécurité de l'actif informationnel est complétée par diverses directives qui viendront préciser les obligations qui en découlent.

Section 1 – Définitions

Dans la présente politique, on entend par :

Confidentialité : le caractère réservé d'une information dont l'accès et la diffusion sont limités aux seules personnes autorisées à la connaître.

Disponibilité : l'aptitude d'un système à assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

Intégrité : la protection de l'exactitude et de l'entièreté de l'information et des méthodes de traitement de celle-ci.

Irrévocabilité : le caractère définitif d'une information. Une information irrévocable ne peut pas être effacée et son annulation ou sa modification est documentée.

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 composants 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 (cellulaire, lecteur MP3, téléphone intelligent, etc.) ; les logiciels, les progiciels, les didacticiels, les documents ou les banques de données et de renseignements (textuelles, sonores ou visuelles) placées dans un équipement ou sur un média informatique ; le système de courrier électronique et le système de messagerie vocale.

Étudiant : toute personne dûment inscrite au secteur régulier ou à la formation continue pour des cours crédités ou non crédités.

Pilote de système : le gestionnaire responsable des aspects opérationnels d'un système corporatif (notamment les systèmes de gestion des dossiers étudiants, de gestion financière, de paie-personnel).

Usager : tout membre du personnel du Collège (cadre, enseignant, professionnel, employé de soutien, etc.), tout étudiant et toute personne physique ou morale autorisée à utiliser les équipements informatiques.

Section 2 – Champ d'application

La présente politique s'applique à toute personne physique ou morale qui utilise ou accède à l'actif informationnel du Collège.

Section 3 – Objectifs

3.1 Protéger l'actif informationnel du Collège

La sécurité concernant les technologies de l'information au sein du Collège vise à permettre la tenue de toutes les activités prévues, dans les meilleures conditions. Dans un souci de protection efficace et de continuité des services, il s'avère nécessaire de prévoir et de mettre en place une telle politique de sécurité visant la confidentialité, l'intégrité et la disponibilité de tous les éléments de l'actif informationnel du Collège.

3.2 Appliquer les bonnes pratiques de sécurité

Les mesures de protection de l'actif informationnel respectent les pratiques de gestion adéquates et généralement reconnues dans le domaine des technologies de l'information. Ces pratiques sont documentées afin de mieux contrôler l'accomplissement des tâches de protection de l'actif informationnel.

3.3 Définir les attentes au regard du comportement des usagers

La protection de l'actif informationnel exige la contribution de tous. Il importe de déterminer les comportements attendus de la part de tous les usagers et d'établir les responsabilités devant être assumées par ceux-ci. Le Collège informe et forme les usagers afin qu'ils contribuent à la gestion sécuritaire des ressources informationnelles.

Section 4 – Dispositions générales

4.1 Utilisation adéquate des outils

Le Collège met à la disposition des usagers des outils de gestion et d'échange d'information qui sont utilisés à des fins professionnelles dans l'exercice de leurs activités reconnues par le Collège.

Le Collège prend les moyens appropriés pour s'assurer d'une utilisation adéquate des éléments de l'actif informationnel par les usagers.

4.2 Mesures de protection

Le Collège 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.

4.3 Protection des renseignements personnels

Les renseignements personnels sont utilisés et ne servent qu'aux fins pour lesquelles ils ont été recueillis ou obtenus. La collecte, 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 en application par le Collège.

4.4 Application de normes reconnues

Le Collège 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.

Section 5 – Mesures de sécurité

5.1 Niveaux de risques et sécurité

Afin de réaliser ses activités, la direction du Collège 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 que tous les usagers utilisent de façon sécuritaire l'actif informationnel.

5.2 Accès aux éléments à l'actif informationnel

Chaque système prévoit des mécanismes permettant d'accorder des droits d'accès différents selon les catégories d'usagers et de vérifier toutes les actions posées sur les données sensibles.

Le droit d'accès d'un usager aux éléments de l'actif informationnel 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 Collège documente les accès donnés à chacun des usagers dans un registre. Ce registre contient notamment, le nom des personnes, leur fonction de travail, les droits qui leur sont attribués et les motifs pour lesquels ces accès sont accordés. Ce registre est mis à jour régulièrement.

Pour chacun des systèmes informationnels, une procédure rigoureuse décrit la gestion des droits d'accès de ses usagers. Chaque accès fait l'objet d'une autorisation formelle par une personne responsable.

5.3 Utilisation de réseaux externes

Le Collège utilise les normes en vigueur afin d'établir la connexion à des réseaux externes et, en particulier, à 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 ou 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 et les correctifs appliqués et le nom du responsable de cet équipement.

5.4 Procédures documentées

Le Collège tient un registre des procédures découlant de la présente politique. Ces procédures sont en lien avec des éléments de l'actif informationnel considérés comme critiques ou sensibles.

5.5 Liste des systèmes de l'actif informationnel

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

5.6 Inventaire de l'actif informationnel

Un inventaire de tous les éléments de l'actif informationnel du Collège 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.

5.7 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 pilote de système concerné.

Section 6 – Partage des responsabilités

6.1 Conseil d'administration du Collège

Le conseil d'administration du Collège adopte la Politique de sécurité de l'actif informationnel.

6.2 Directeur général

Le directeur général du Collège est responsable de l'application de la présente politique.

6.3 Responsable des technologies de l'information

Le responsable des technologies de l'information :

- accompagne les gestionnaires dans la mise en place des processus de sécurité ;
- assure, au besoin, la coordination entre les diverses directions du Collège 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 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.

6.4 Pilote de système

Le gestionnaire appelé « pilote de système » :

- applique et fait appliquer par le personnel sous sa responsabilité 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 ;
- rédige les procédures concernant le système dont il est responsable ;
- accorde les accès à chacun des usagers et tient un registre décrivant ceux-ci ;
- vérifie la cohérence des accès selon les statuts définis pour chacun des usagers et les exigences de la présente politique.

6.5 Gestionnaires

Les gestionnaires du Collège :

- informent leurs employés de la politique, des directives et des procédures concernant la sécurité des technologies de l'information ;
- s'assurent que leurs employés mettent en pratique les directives émises par le Collège.

6.6 Usagers

Les usagers :

- prennent connaissance, appliquent et respectent la Politique de sécurité de l'actif informationnel, les directives qui en découlent, les normes et les procédures du Collège, les lois et les règlements relatifs à la sécurité des technologies de l'information ;
- sont responsables des actions résultant de l'usage de leur identifiant, de leur code d'accès ou de leur mot de passe, que ces actions soient posées par eux-mêmes ou par un tiers.
- avisent une personne responsable, leur professeur ou leur supérieur immédiat, de toute situation susceptible de compromettre la sécurité de l'actif informationnel.

Section 7 – Divers

7.1 Révision de la politique

La présente politique sera révisée au besoin, au plus tard dans une période de cinq à sept ans suivant l'adoption par le conseil d'administration du Collège. Lors de la revue de la présente politique, il importe de réévaluer les moyens mis en œuvre afin de répondre aux préoccupations de sécurité.

7.2 Sanction

Le non-respect d'un élément de cette politique ou des directives qui en découlent est soumis au processus de sanctions prévu, notamment au règlement n^{o} 14 relatif au traitement des plaintes, des sanctions et des mécanismes de recours et d'appel, ou aux conventions collectives.

7.3 Entrée en vigueur

La présente politique entre en vigueur le jour de son adoption par le conseil d'administration du Collège.

---

* Adoptée par le Conseil d'administration le 22 février 2010.

Document certifié conforme

Linda Chartrand
Secrétaire du conseil