CÉGEP TROIS-RIVIÈRES

RÈGLEMENT
✓ ***POLITIQUE***
PROCÉDURE

POLITIQUE CONCERNANT L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DES TÉLÉCOMMUNICATIONS

Adoptée par le conseil d'administration le 28 juin 2010
Règlement R-604 modifié en politique au conseil d'administration du 24 février 2016

PRÉAMBULE

Le Cégep de Trois-Rivières reconnaît l'importance pour les membres de la communauté collégiale d'avoir accès à ses équipements, ses ressources informatiques et de télécommunication ainsi qu'à son réseau informatique, pour la réalisation d'activités d'enseignement, d'apprentissage, de recherche, de gestion, d'administration et de services à la collectivité reliées à la réalisation de la mission du Collège.

En tant que propriétaire et gestionnaire d'équipements et de ressources informatiques et de télécommunication, le Collège doit s'assurer que leur utilisation et le traitement de l'information ainsi que l'utilisation du réseau soient conformes à certaines normes.

Au-delà des dispositions contenues dans la présente politique, le Collège s'attend à ce que la conduite de chaque utilisateur soit dictée par les règles usuelles de bienséance, de courtoisie et par les politiques, règlements et procédures en vigueur au Collège ainsi que par les lois et règlements en vigueur au Canada et dans la province de Québec.

CHAMP D'APPLICATION

La présente politique s'applique :

- au personnel régulier et occasionnel du Collège, aux étudiantes, aux étudiants et aux autres utilisateurs dûment autorisés des équipements informatiques du Collège;

- à tout actif informatique et de télécommunication, peu importe sa localisation, appartenant ou non au Collège, mais utilisé dans ses locaux;

- à toute donnée saisie, traitée ou emmagasinée avec des équipements informatiques du Collège dans le cadre de ses activités d'enseignement, de recherche, de gestion et de services à la collectivité.

ARTICLE 1 – OBJECTIFS

La présente politique établit le cadre administratif régissant l'utilisation de tous les équipements informatiques (logiciels, postes de travail informatiques, réseaux de communication, données informatiques, etc.) du Collège. Il vise le respect des lois et des règlements concernant les technologies de l'information. Il touche aussi la protection des investissements collectifs contre les utilisations abusives ou illégales de la part des utilisateurs. Finalement, il définit les comportements adéquats et socialement acceptables attendus des utilisateurs.

ARTICLE 2 – DÉFINITIONS

Dans cette politique, à moins que le contexte n'impose un sens différent, les expressions et les termes suivants signifient :

2.1 Collège : Le Cégep de Trois-Rivières.

2.2 DSI : La Direction des services informatiques.

2.3 Équipement informatique : Les composants et les équipements réseaux, les serveurs informatiques, les ordinateurs centraux, les mini-ordinateurs, les micro-ordinateurs, 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 et tout équipement de télécommunication (commutateurs, routeurs, réseau filaire, etc.), les logiciels, les progiciels, les didacticiels, les documents ou les banques de données et d'information textuelle, sonore ou visuelle placées dans un équipement ou sur un média informatique, le système de courrier électronique et le système de messagerie vocale, dont le Collège est propriétaire ou locataire, ou sur lesquels il possède un droit d'utilisation.

2.4 Étudiant : Toute personne inscrite officiellement au Collège, tant au secteur de l'enseignement régulier qu'à la formation continue.

2.5 Matériel piraté : Tout logiciel, progiciel, didacticiel, média numérique de nature textuelle, sonore ou visuelle, toute banque de données et d'information distribués de façon commerciale et installés sur les équipements informatiques du Collège et dont celui-ci n'a pas les droits d'utilisation.

2.6 Utilisateur : Tout membre du personnel du Collège (cadres, enseignants, professionnels, employés de soutien, formateurs-chercheurs, employés dont les tâches ne sont pas visées par un certificat d'accréditation) tout étudiant, ainsi que toute personne physique ou morale autorisée à utiliser les équipements informatiques.

2.7 Réseau informatique : Ensemble d'équipements informatiques interconnectés par des liens de télécommunications filaires ou sans fil permettant d'échanger de l'information.

2.8 Mandataires de la DSI : Personnes, services ou départements dûment autorisés à procéder à des interventions sur les équipements informatiques du Collège.

ARTICLE 3 – RESPONSABILITÉS DE L'UTILISATEUR

3.1 Accessibilité

Seuls le personnel, les étudiants et les autres utilisateurs dûment autorisés peuvent avoir accès et utiliser les équipements et les ressources informatiques et de télécommunication ou le réseau et ce, dans les limites de l'autorisation accordée aux utilisateurs par le Collège.

Si l'utilisateur ne respecte pas les règles d'utilisation de la présente politique, il peut se voir retirer cette autorisation.

3.2 Protection des données appartenant à l'utilisateur

L'utilisateur est responsable de ses données enregistrées sur les unités non réseau du poste de travail informatique du Collège. Il doit voir, lui-même, à la conservation de copies de sauvegarde de ses documents informatiques. Il ne peut invoquer la responsabilité du Collège pour la perte d'un fichier ou sa destruction.

3.3 Utilisation des équipements informatiques

Toute utilisation des équipements informatiques pour des usages non autorisés, illégaux ou commerciaux, est strictement interdite.

Les jeux électroniques, le clavardage ou toutes autres utilisations (films, vidéos, musique, etc.) des équipements informatiques peuvent être autorisés exclusivement dans le cadre des activités d'enseignement, d'apprentissage et de recherche.

L'utilisation des équipements informatiques appartenant au Collège afin de réaliser ou de tenter de réaliser une fraude informatique ou une utilisation malveillante est interdite.

Il est strictement interdit de poser tout acte pouvant nuire au bon fonctionnement des équipements informatiques, entre autres, par l'insertion et la propagation de virus informatiques ou par la destruction ou la modification de données ou de logiciels.

Il est interdit de modifier ou de détruire sciemment un logiciel, une banque de données ou un fichier électronique, ou d'y accéder sans l'autorisation de son propriétaire.

3.4 Matériel piraté

L'utilisation, l'installation, le téléchargement, la copie et le recel de matériel piraté sont interdits. La participation à de tels actes constitue une action illégale.

Les reproductions de logiciels doivent être réalisées par la DSI ou ses mandataires selon les normes de la licence d'utilisation desdits logiciels.

3.5 Modification des systèmes informatiques

Tous les logiciels, incluant les jeux, les logiciels de sauvegarde d'écrans, les logiciels de démonstration, les barres d'outils, les gratuiciels ou les polices de caractères sur un poste de travail informatique du Collège doivent être approuvés et installés par la DSI ou ses mandataires.

La modification ou l'altération des fonctions du système d'exploitation ou d'un logiciel d'application ne peut se faire que par la DSI ou ses mandataires.

3.6 Modification matérielle des équipements informatiques

Aucun ajout ou modification aux équipements informatiques n'est permis sans la supervision de la DSI ou ses mandataires.

Il est formellement interdit d'ajouter ou de retirer, même de manière temporaire, des composants à un équipement informatique appartenant au Collège. De même, il est interdit de brancher des équipements personnels dans les prises réseau déjà utilisées par les équipements du Collège.

Toutefois, l'utilisation de périphériques de stockage personnels (clé USB ou autres) est autorisée.

L'utilisateur a la responsabilité de laisser le matériel informatique et ses composants en état de marche et en sécurité et d'en rapporter, le cas échéant, les anomalies au centre d'appel de la DSI.

3.7 Téléchargement de logiciels, de données ou de documents multimédias

Le téléchargement de données, de logiciels ou de documents multimédias est permis dans la mesure où le contenu est utilisé à des fins pédagogiques, d'apprentissage, de recherche ou de gestion. Tout autre usage est interdit. Cette restriction vise, dans un souci d'équité entre les utilisateurs, à permettre à tous les utilisateurs de bénéficier d'un accès Internet rapide en minimisant l'engorgement de la bande passante.

3.8 Utilisation du réseau Internet à des fins personnelles sur les heures de travail

Il est interdit aux employés du Collège d'utiliser Internet à des fins personnelles sur les heures de travail. Toutefois, une utilisation à des fins personnelles et non commerciales est tolérée en dehors des heures de travail.

3.9 Sabotage des équipements informatiques

Tout acte de sabotage des équipements informatiques ou des données conservées sur le réseau informatique du Collège constitue une action illégale.

ARTICLE 4 – RESPONSABILITÉS DU COLLÈGE

4.1 Confidentialité de l'information

Le Collège est tenu de protéger les messages électroniques, les fichiers et les espaces de sauvegarde dédiés aux utilisateurs sur le réseau de l'intrusion de personnes non autorisées.

4.2 Sécurité des données sur le réseau

Le Collège doit prendre des mesures de sauvegarde adéquates pour protéger les documents ou les données déposés sur le réseau par les utilisateurs.

Dans le cas des applications de gestion du Collège, la DSI effectue, de manière régulière, des copies de sauvegarde permettant d'assurer la sécurité et l'intégrité des données.

Dans le cas des unités réseau, la DSI effectue, de manière régulière, des copies de sauvegarde permettant de restaurer les données des utilisateurs lors d'un problème technique.

En ce qui a trait aux données des utilisateurs enregistrées sur des unités réseau de sous-traitants informatiques, la DSI voit à obtenir de manière contractuelle des garanties de sécurité et d'intégrité des données. À cet égard, les fournisseurs informatiques sont tenus d'appliquer les règles de l'art dans la gestion des données qu'ils traitent.

4.3 Protection des systèmes informatiques

La DSI doit instaurer des mesures de contrôle et de sécurité appropriées pour protéger adéquatement les équipements informatiques sous sa responsabilité. Elle administre ses équipements de manière licite et efficace en respectant le caractère confidentiel de l'information des utilisateurs lors de toute intervention de gestion.

4.4 Renseignements protégés

L'information contenue dans les équipements informatiques de même que sur le réseau est confidentielle lorsqu'elle a le caractère d'un renseignement nominatif ou le caractère d'un renseignement relatif à la vie privée de la personne au sens du Code civil du Québec. Elle est protégée et n'est accessible que par les personnes mandatées par le Collège.

4.5 Protection contre les virus

Le Collège a l'obligation de mettre en place des outils permettant la vérification de la présence de virus dans ses systèmes.

4.6 Vérification

Une vérification des équipements informatiques nécessitant la lecture des informations personnelles et privées d'un utilisateur ne peut être effectuée qu'après avoir prévenu la personne concernée et lui avoir donné l'occasion de préserver ses données. Lorsque la DSI a des motifs raisonnables de soupçonner un usage frauduleux des équipements informatiques, elle est autorisée, et ce, accompagnée d'un témoin qui occupe un poste de cadre à la Direction des ressources humaines, à procéder sans préavis aux vérifications nécessaires des équipements informatiques afin de s'assurer du respect des politiques, règlements et procédures du Collège, et des lois et règlements provinciaux ou fédéraux.

ARTICLE 5 – ACCÈS AUX ÉQUIPEMENTS INFORMATIQUES

5.1 Accès à l'ensemble des équipements informatiques

5.1.1 Exclusivité

Les équipements informatiques sont mis à la disposition des seuls utilisateurs autorisés pour la réalisation d'activités d'enseignement, d'apprentissage, de recherche, de gestion et d'administration reliées à la réalisation de la mission éducative du Collège et de services à la collectivité.

5.1.2 Droit à la confidentialité

L'utilisateur a droit à la confidentialité de l'information qui lui est propre et qui n'appartient pas au Collège, qu'elle soit enregistrée sur son poste de travail informatique, sur le réseau du Collège ou dans sa boîte de courrier électronique.

L'utilisateur perd ce droit de confidentialité lorsqu'il emploie les équipements informatiques en contravention aux politiques, règlements et procédures du Collège, ou aux lois et règlements provinciaux ou fédéraux.

5.1.3 Respect des mécanismes de sécurité

L'utilisateur doit respecter les mécanismes de sécurité des fichiers, des banques de données, des ordinateurs, des systèmes ou des réseaux et ne pas tenter de les percer.

5.1.4 Messages ou documents à caractère obscène, pornographique, diffamatoire, haineux ou proférant des menaces

Il est strictement interdit de capter volontairement, de stocker, de reproduire ou de transmettre au moyen des équipements informatiques un document ou un message à caractère obscène, pornographique, diffamatoire, haineux ou proférant des menaces.

5.1.5 Retrait de l'autorisation d'accès

Lorsque le Collège retire le droit d'utilisation des équipements informatiques pour quelque raison que ce soit, les données et les programmes de l'utilisateur sont considérés comme périmés après un délai de 30 jours à compter de la date du retrait de l'autorisation par le Collège. La DSI aura le droit de les supprimer sans droit de recours par l'utilisateur.

5.2 Accès à un poste de travail informatique

5.2.1 Poste de travail informatique

La personne utilisant un poste de travail informatique doit se conformer aux directives données de temps à autre par la DSI.

5.2.2 Accès aux laboratoires informatiques

Les locaux servant de laboratoire informatique sont accessibles uniquement aux étudiants inscrits au Collège, aux membres du personnel concernés et à toute personne ayant obtenu une autorisation du Collège.

L'utilisateur doit respecter les horaires d'ouverture, la disponibilité et le caractère dédié des laboratoires informatiques.

Il est interdit de boire ou de manger dans les laboratoires informatiques.

5.2.3 Déplacement des équipements

Il est formellement interdit pour quiconque de déplacer les ordinateurs ou les périphériques d'un local sans l'autorisation de la DSI.

5.3 Accès aux réseaux

5.3.1 Code d'accès réseau

Un code d'accès réseau et un mot de passe sont alloués à un utilisateur par le Collège. Le mot de passe fourni à l'utilisateur est strictement confidentiel. L'utilisateur est responsable des communications effectuées par l'utilisation de son code d'accès et il doit voir à protéger le caractère confidentiel de son mot de passe. Au besoin, il doit changer lui-même son mot de passe en utilisant la procédure fournie par la DSI.

L'utilisateur ne peut, en aucun cas, communiquer, transmettre ou dévoiler son mot de passe à un autre utilisateur ou à un tiers. Il ne peut permettre à des tiers d'accéder aux équipements informatiques par son compte à moins d'entente avec la DSI.

5.3.2 Expiration du code d'accès réseau

Un étudiant doit être inscrit au Collège pour que son code d'accès réseau soit actif. Lorsqu'un étudiant n'est plus inscrit, depuis deux sessions consécutives, son mot de passe réseau, son espace de stockage et ses fichiers personnels sont détruits. S'il se réinscrit, son code d'accès réseau sera réactivé et un nouveau mot de passe réseau lui sera alloué.

5.3.3 Accès non autorisé

Il est interdit à un utilisateur d'accéder ou de tenter d'accéder à des fichiers, des banques de données, des systèmes, des réseaux internes ou externes dont il n'a pas les droits d'accès.

5.3.4 Accès aux données

L'absence de restrictions d'accès à des données ne suppose pas nécessairement pour un utilisateur le droit de les consulter. L'utilisateur doit s'abstenir de consulter ou de copier des données accessibles qui ne lui sont pas destinées, à moins qu'il ne soit évident que ces données soient de nature publique.

5.3.5 Transmission de documents confidentiels

L'utilisateur doit faire usage de mesures de protection et de sécurité adéquates lors de la transmission de documents, de données de gestion ou d'information protégés en vertu de la Loi sur l'accès à l'information.

5.3.6 Usurpation d'accès

Dans toute communication, l'utilisateur doit s'identifier avec son code d'accès réseau et son mot de passe et en aucun cas il ne peut usurper ou tenter d'usurper l'identité d'un autre utilisateur ou celle d'un tiers.

5.3.7 Décryptage des mots de passe

Il est strictement interdit à un utilisateur de tenter de décrypter ou de découvrir le mot de passe associé à un code d'accès réseau.

5.3.8 Modification de la configuration du réseau

Il est interdit d'ajouter ou de modifier des composants au réseau du Collège sans une autorisation de la Direction des services informatiques. Les équipements comme les routeurs filaires ou sans fil font partie de cet interdit.

5.3.9 Branchement au réseau du Collège

Lorsqu'un utilisateur se branche au réseau du Collège (réseau filaire ou réseau sans fil), le Collège se réserve le droit de déconnecter tout utilisateur faisant une

utilisation inappropriée du réseau ou propageant de manière volontaire ou involontaire des logiciels malveillants pouvant causer des problèmes à d'autres utilisateurs ou à des équipements informatiques du Collège.

Sont considérés comme des logiciels malveillants les logiciels suivants : virus, vers (worms), wabbits, les chevaux de Troie (Trojan horses), les portes dérobées (backdoors), les logiciels-espions (spywares), les renifleurs de paquets (packet sniffers), les enregistreurs de frappe (keyloggers), les composeurs (dialers), les publiciels (adwares), les canulars (hoax), les logiciels d'hameçonnage (phishing) et tout autre logiciel qui s'installent ou s'exécutent sur une machine hôte sans l'autorisation du Collège.

5.3.10 Interception des communications

Il est formellement interdit de récupérer des trames de données transitant sur le réseau du Collège à l'aide de logiciels renifleurs de paquets (packet sniffers). L'écoute d'un réseau informatique afin de récupérer à la volée de l'information non chiffrée constitue une infraction.

5.4 Utilisation de la messagerie électronique

L'utilisation du courrier électronique doit être reliée prioritairement au travail ou aux études de l'utilisateur. Il est interdit d'envoyer des messages non sollicités, des messages en chaîne ou tout autre type d'usage qui peut provoquer un engorgement du réseau.

Pour tous les courriels diffusés sur le réseau, l'utilisateur doit s'identifier à titre de signataire du message et préciser, s'il y a lieu, à quel titre il s'exprime. Il est interdit d'utiliser un ou des subterfuges ou d'autres moyens pour transmettre du courrier électronique de façon anonyme ou au nom d'une autre personne.

L'utilisateur doit rédiger ses messages électroniques diffusés sur le réseau dans un langage courtois. Il est interdit d'utiliser un vocabulaire injurieux, malveillant, haineux ou discriminatoire, ainsi que toute forme de harcèlement, de menace ou de diffamation.

ARTICLE 6 – SANCTIONS PRÉVUES

Le Collège se réserve le droit de retirer l'autorisation d'utilisation des équipements informatiques et d'interdire l'accès à ses équipements à quiconque ne respecte pas les règles d'utilisation ou cause, par une utilisation abusive, des dommages aux équipements informatiques.

Des plaintes et des réclamations en dommages pourront être portées devant la justice contre toute personne tenue responsable de gestes relevant d'une utilisation malveillante ou illégale des équipements informatiques du Collège.

Lorsqu'un utilisateur commet une infraction à la présente politique concernant l'utilisation des technologies de l'information et des communications du Collège, il est

soumis au processus de sanctions du Collège prévu au Règlement numéro R-102 relatif aux conditions de vie au Collège. De plus, selon la nature de l'infraction, il pourrait être passible de poursuite au civil ou au criminel.

ARTICLE 7 – APPLICATION DE LA POLITIQUE

Le directeur général désigne le directeur des services informatiques comme responsable de l'application de cette politique et de sa révision. En plus d'administrer l'application des différentes règles d'utilisation, le directeur des services informatiques est chargé de la sensibilisation des différents utilisateurs du Collège en regard des comportements attendus.

ARTICLE 8 – ENTRÉE EN VIGUEUR

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