Collège Lionel-Groulx

POLITIQUE DE SÉCURITÉ INFORMATIQUE

L’utilisation du genre masculin dans ce document sert uniquement à alléger le texte et désigne autant les hommes que les femmes

Table des matières

1. Objet de la politique 4
2. Cadre légal et règlementaire 4
3. Cadre normatif 4
4. Définitions 4
5. Champ d'application de la politique 5
6. Les objectifs visés 5
7. Documents à l'appui de la politique 5
8. Propriété des données 6
9. Classification de l'information 6
10. Accès aux technologies de l'information 6
    10.1 Code d'accès et mot de passe 7
    10.2 Accès à distance 7
11. Accès aux applications 8
    11.1 Les applications administratives 8
    11.2 Les applications reliées aux activités d'enseignement 8
12. Impartition et tiers 8
13. Exigences 8
    13.1 Programme de sécurité 8
    13.2 Formation et sensibilisation 9
    13.3 Analyse proactive des menaces technologiques 9
    13.4 Utilisation du courrier électronique et d'internet 9
    13.5 Sécurité des installations informatiques 10
    13.6 Sécurité physique de l'espace de travail 10
    13.7 Acquisition et entretien de matériels et de logiciels 10
    13.8 Copie de sécurité 11
    13.9 Continuité des opérations 11
    13.10 Enquêtes sur les incidents de sécurité 11
14. Sanctions 11
15. Responsabilités 12
16. Examen 12
17. Entrée en vigueur et abrogation 12

1. OBJET DE LA POLITIQUE

La présente politique constitue le cadre général concernant les accès, l'utilisation et la sécurité des technologies de l'information du Collège Lionel-Groulx. Elle oriente les comportements attendus des usagers quant à l'utilisation du matériel informatique, des logiciels, les accès et l'utilisation du réseau informatique (intranet et extranet).

Cette politique souligne l'importance d'assurer les opérations électroniques pour une prestation de services de qualité. Cette politique permet de préserver la confidentialité, la disponibilité, l'intégrité et la valeur des biens.

2. CADRE LÉGAL ET RÈGLEMENTAIRE

- La Chartre des droits et libertés de la personne (L.R.Q.,c.C-12);
- Le Code civil du Québec (L.Q. 1991, c C-64);
- La Loi sur les droits d'auteur (L.R.C., C-42);
- Le Code criminel (C-46);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., C.A-2.1);

3. CADRE NORMATIF

La présente politique s'appuie sur la norme internationale ISO/CEI 27002 :2005, *Techniques de sécurité : Code de bonne pratique pour la gestion de la sécurité de l'information.*

4. DÉFINITIONS

Quelques définitions en regard de la terminologie sont proposées ici aux fins de cette politique.

Collège désigne la personne morale qu'est le Collège Lionel-Groulx, collège d'enseignement général et professionnel au sens de la Loi sur les collèges d'enseignement général et professionnel.

Propriétaire désigne une direction, un service ou une unité administrative qui est le principal utilisateur d'une application et dont il est l'ultime responsable (imputable) de son utilisation et du traitement de l'information y découlant.

Rustine désigne un programme destiné à corriger les défauts, les bogues d'un logiciel.

5. CHAMP D'APPLICATION DE LA POLITIQUE

La présente politique s'applique sans exception au personnel, aux élèves, organismes et à tous les tiers utilisant les installations technologiques du Collège.

La politique énonce les principes qui permettent aux utilisateurs d'obtenir les accès requis pour leur permettre d'effectuer leurs travaux.

6. LES OBJECTIFS VISÉS

Cette politique vise les objectifs suivants :

- D'assurer que les utilisateurs observent les bonnes pratiques et les règles quant à l'utilisation des technologies de l'information;
- D'assurer que les normes en matière de sécurité informatique soient dûment mises en application
- De réviser périodiquement les résultats des vérifications et contrôles, notamment pour y relever les anomalies et autres incidents
- De recommander les actions à prendre pour corriger les situations anormales ou dangereuses, notamment, les processus opérationnels et les grandes stratégies en matière informatique et les achats d'équipement.
- D'informer le comité de Direction du Collège des travaux, activités et incidents en matière de sécurité informatique.
- D'assurer que les éléments opérationnels qui requièrent une approbation des différentes directions soient respectés.

7. DOCUMENTS À L'APPUI DE LA POLITIQUE

La présente politique vient chapeauter les directives, les règles et les règlements déjà approuvés par les différentes instances (le conseil d'administration, le comité exécutif, Comité de Direction du Collège).

8. PROPRIÉTÉ DES DONNÉES

Toute information de nature administrative installée dans les ressources informatiques du Collège est la propriété unique du Collège, sauf les informations assujetties à la Loi sur les droits d'auteur (L.R.C., C-42), et les documents produits par les enseignants et les étudiants dans le cadre des activités pédagogiques.

Il est interdit de poser un acte visant à détruire ou porter atteinte à l'intégrité des données des autres utilisateurs des ressources informatiques ou des données d'autres organismes.

9. CLASSIFICATION DE L'INFORMATION

L'attribution de la classification revient aux gestionnaires des services (propriétaire), qui eux, détermineront les droits d'accès accordés aux usagers sous leur responsabilité. Une information peut être catégorisée sous trois grandes classes en respect de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., C.A-2.1) :

a) Publique

Cette information peut être distribuée sans restriction à l'intérieur comme à l'extérieur du collège. Elle est généralement informative. Sa divulgation ne risque pas de causer des dommages ou préjudices au collège.

b) Privée

Cette information est strictement d'usage interne. Les utilisateurs peuvent s'en servir pour effectuer leur travail. Il pourrait y avoir des impacts indirects sur le collège si les informations de cette classe étaient dévoilées au public.

c) Confidentielle

L'information de cette catégorie doit être protégée par des obligations légales ou contractuelles. Elle est généralement stratégique. Elle nécessite le plus haut niveau de sécurité. Sa divulgation pourrait causer des dommages importants au Collège.

10. ACCÈS AUX TECHNOLOGIES DE L'INFORMATION

L'accessibilité au réseau entraine une certaine responsabilité pour les utilisateurs. Ceux-ci doivent respecter les différents règlements, directives et les objectifs visés quant à l'accès et l'utilisation des technologies de l'information mises à leur disposition.

Respectant ces principes d'imputabilité, la règle générale inhérente à l'attribution d'un code d'accès est : ***Un utilisateur, un code d'accès personnel et aucun code d'accès générique.***

10.1 Code d'accès et mot de passe

Tout personnel, incluant les enseignants, doit obligatoirement être inscrit aux registres de la Direction des ressources humaines pour obtenir un code d'accès aux ressources technologiques du Collège. Les ressources technologiques sont attribuées en fonction des tâches et des activités.

Tout étudiant doit être inscrit au Collège pour obtenir un code d'accès aux services technologiques. Tout comme les membres du personnel, les accès aux ressources principales sont désactivés dès la fin de leurs études au collège et/ou dès la cessation du lien d'emploi pour ce qui est du personnel.

Les accès aux systèmes doivent être maintenus à jour promptement lors des mutations et des départs. La Direction de l'informatique, des technologies de l'information et des communications conjointement avec la Direction des ressources humaines met en place des mesures de contrôles appropriées pour faciliter la communication lors des arrivées, des départs et des mutations du personnel.

Le choix des mots de passe, leur utilisation et leur gestion répondent aux normes de l'industrie.

L'utilisation du réseau, y compris le réseau sans fil, est strictement contrôlée pour prévenir l'usage non autorisé des équipements. La direction de l'informatique, des technologies de l'information et des communications configure le matériel et les logiciels correctement contre les tentatives d'intrusion.

10.2 Accès à distance

La direction de l'informatique, des technologies de l'information et des communications doit assurer les procédures visant à:

a) Configurer le réseau pour assurer un niveau suffisant de performance et de fiabilité dans le but de répondre aux exigences en matière de la sécurité des systèmes.

b) Configurer le matériel et les logiciels d'accès à distance correctement contre les tentatives d'intrusion;

c) Contrôler l'accès à distance par des techniques robustes d'identification, d'authentification et de chiffrage;

d) Accorder l'accès à distance aux utilisateurs ou tiers qui en ont besoin dans le cadre de leurs fonctions seulement.

11. ACCÈS AUX APPLICATIONS

Le code d'accès au réseau du Collège assure l'accès à des ressources de base, et il ne garantit pas les accès aux applications nécessaires à l'exercice des activités. Dans cette perspective, la direction de l'informatique, des technologies de l'information et des communications conjointement avec les directions et services s'assurent que chaque utilisateur ait accès aux ressources informationnelles nécessaires pour exercer ses fonctions.

11.1 Les applications administratives

Les accès aux applications informatiques administratives sont définis par le propriétaire principal de chaque application stratégique. Ce dernier est l'ultime responsable de l'accès à son application.

Les droits d'accès et les rôles sont autorisés par le propriétaire. Le processus d'identification et d'autorisation des accès d'une application logiciel est formel, soit par écrit, soit via un logiciel utilisé à cette fin. Les accès définis dans le système et dans l'infrastructure sont conformes aux autorisations indiquées par le propriétaire de l'application et une révision périodique des droits d'accès devra avoir lieu minimalement tous les ans.

11.2 Les applications reliées aux activités d'enseignement

De facto, les enseignants, étudiants et personnels de soutien en lien avec les activités pédagogiques ont automatiquement accès aux services technologiques reliés à cette sphère d'activité.

12. IMPARTITION ET TIERS

La présente politique s'applique autant aux processus impartis qu'aux opérations internes du Collège. Les tiers sont tenus de satisfaire aux exigences de cette politique, des normes de sécurité, de la documentation technique et des procédures de sécurité au même titre que le personnel du Collège.

Chaque accès par des tiers aux applications logicielles stratégiques est autorisé par la direction de l'informatique des technologies de l'information et des communications et est dûment consigné dans un registre administré par celle-ci.

13. EXIGENCES

Les utilisateurs doivent satisfaire aux exigences de base de cette politique, des normes en matière de sécurité, de la documentation technique et des procédures de sécurité.

13.1 Programme de sécurité

La politique donne le mandat à la direction de l'informatique, des technologies de l'information et des communications d'établir un programme de sécurité qui assure la

coordination de toutes les fonctions de la politique et la mise en oeuvre de ses exigences. Ces fonctions comprennent l'administration générale, la formation et sensibilisation, l'identification des biens, la gestion des risques de la sécurité, le contrôle de l'accès, les vérifications de fiabilité et de sécurité, la sécurité matérielle, la sécurité des technologies de l'information, la sécurité en cas d'urgence et de menace accrue, la planification de la continuité opérationnelle et les enquêtes sur les incidents de sécurité.

Les utilisateurs sont tenus de rapporter promptement à la Direction les incidents de sécurité et le non-respect de la politique par un utilisateur.

13.2 Formation et sensibilisation

La direction de l'informatique, des technologies de l'information et des communications doit :

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

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

13.3 Analyse proactive des menaces technologiques

La direction de l'informatique, des technologies de l'information et des communications doit sauvegarder les systèmes électroniques d'information jugés comme étant essentiels contre les menaces qui changent rapidement et qui ont le potentiel d'affecter la confidentialité, l'intégrité, la disponibilité, l'usage prévu et la valeur des systèmes.

L'approche utilisée tient compte des changements qui peuvent être soudains et devra soutenir la prestation continue de services. Ceci exige que la direction de l'informatique, des technologies de l'information et des communications procède à des contrôles sécuritaires de base permettant une surveillance continuelle afin d'identifier et d'analyser les menaces et d'établir des mécanismes efficaces face à de telles circonstances.

13.4 Utilisation du courrier électronique et d'internet

La direction s'assure de mettre en place des mesures pour protéger le réseau du Collège 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.

Le téléchargement d'information à partir d'internet et l'ouverture des attachements de courriers électroniques doivent être faits avec soin pour limiter l'exécution de code malveillant.

Le courrier électronique et Internet sont strictement utilisés pour les besoins du Collège. Les fichiers joints aux messages sont envoyés avec discernement pour éviter de transmettre l'information classifiée et protégée.

13.5 Sécurité des installations informatiques

La direction de l'informatique, des technologies de l'information et des communications délimite les aires à accès restreint et installe les systèmes de sécurité ainsi que le matériel nécessaire selon une évaluation des menaces et des risques

La direction s'assure également de mettre en place les mesures nécessaires pour protéger les équipements et l'information qu'ils contiennent.

La direction 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 leur mise au rebus

13.6 Sécurité physique de l'espace de travail

Il est strictement interdit d'utiliser le matériel informatique à d'autres fins que celles utilisées pour les besoins du Collège seulement. La direction de l'informatique, des technologies de l'information et de communications s'assure du maintien de mesures suffisantes pour sécuriser les postes de travail laissés sans surveillance.

Les utilisateurs doivent prendre des mesures appropriées pour protéger adéquatement les renseignements classifiés et protégés en leur possession.

13.7 Acquisition et entretien de matériels et de logiciels

Toute acquisition de produit matériel ou logiciel est approuvée par la direction de l'informatique, des technologies de l'information et des communications. En ce sens, elle s'assure que:

a) L'acquisition de nouveaux produits commerciaux est compatible avec les orientations du Collège;

b) L'acquisition et le développement des nouveaux produits tiennent compte des exigences de sécurité;

c) Les nouveaux produits sont compatibles avec les systèmes en place;

d) Les produits utilisés sont dûment enregistrés;

e) Les nouveaux logiciels et les rustines sont appliqués seulement après avoir été testés et approuvés par le propriétaire de l'application.

13.8 Copie de sécurité

La direction de l'informatique, des technologies de l'information et des communications met en place des mesures suffisantes pour protéger l'actif informationnel du Collège. Elle met en place une procédure de sauvegarde et de recouvrement, effectue des tests de recouvrement à intervalle régulier, conserve les copies dans un lieu physique distinct et effectue régulièrement un suivi sur le matériel de sauvegarde

13.9 Continuité des opérations

Pour assurer la prestation continue des services essentiels, la direction de l'informatique, des technologies de l'information et des communications prépare un plan de continuité pour les TI dans le cadre de la planification de la continuité opérationnelle de ses activités de recouvrement suite à un incident. Ce plan doit prévoir :

a) Une structure définissant les autorités et les responsabilités pour le développement et l'approbation du plan de continuité;

b) Une analyse d'impact pour inventorier par ordre de priorité les services et les biens essentiels;

c) Des plans, des mesures et des préparatifs pour assurer la disponibilité continue des services et des biens essentiels, et de tout autres services ou bien tel qu'indiqué par une évaluation des menaces et des risques;

d) Des activités de revue, de mise à l'essai et de vérifications du plan de continuité.

La direction de l'informatique, des technologies de l'information et des communications applique un mécanisme de redondance des composantes critiques et un entretien régulier de l'équipement pour assurer la prestation continue des services essentiels lors d'une panne, sans devoir recourir systématiquement au plan de continuité des opérations.

13.10 Enquêtes sur les incidents de sécurité

La direction de l'informatique, des technologies de l'information et des communications implante des procédures de compte rendu et d'enquête relativement aux incidents de sécurité et prend des mesures correctives pour y donner suite.

14. SANCTIONS

Toute contravention à la présente politique, y compris aux règles, règlements ou directives découlant de ladite politique, peut mener à la suspension des privilèges d'accès aux technologies de l'information du Collège. Des mesures administratives, disciplinaires ou légales pourront être enclenchées auprès des contrevants.

15. RESPONSABILITÉS

Chaque direction et unité administrative en collaboration avec la Direction informatique des technologies de l'information et des communications est responsable de l'application et du respect de la présente politique.

16. EXAMEN

La présente politique sera réexaminée au besoin.

17. ENTREE EN VIGUEUR ET ABROGATION

La présente Politique a été adoptée par le conseil d'administration du 15 juin 2010 et est entrée en vigueur le jour de son adoption.

La présente Politique abroge tout autre document ou texte adopté antérieurement portant sur les mêmes objets.