Collège Lionel-Groulx

RÈGLEMENT SUR LES CONDITIONS D'UTILISATION DES RESSOURCES INFORMATIONNELLES

Adoption au conseil d'administration du 28 novembre 2017

TABLE DES MATIÈRES

1. DÉFINITIONS

1.1 Définitions

Actifs informationnels :	Tous éléments contenant de l'information ayant une valeur pour le gouvernement ou pour l'organisation. Fait aussi référence à des biens physiques tels que les appareils, systèmes, téléphones, support de toutes natures, bases de données, logiciels, etc.
Collège :	Désigne la personne morale Collège Lionel-Groulx.
CSGI :	Désigne le Coordonnateur Sectoriel de la Gestion des Incidents.
DG :	Désigne la Direction générale.
DIIM :	Désigne la Direction des Infrastructures Informationnelles et Matérielles.
DRH :	Désigne la Direction des Relations Humaines.
Propriétaire :	Désigne, tel que défini dans la *Politique sur la sécurité de l'information* (chapitre 10.7) le gestionnaire détenant l'autorité au sein d'un service 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.
RSI :	Désigne le Responsable de la Sécurité de l'Information.
Rustine :	Désigne un programme destiné à corriger les défauts, les bogues d'un logiciel.
Utilisateur :	Désigne toute personne physique ou morale qui utilise les actifs informationnels.
TI :	Désigne l'ensemble des équipements, logiciels et services utilisés pour la collecte, le traitement et la transmission de l'information.

2. OBJET DU RÈGLEMENT

Le présent Règlement constitue le cadre de référence en ce qui concerne les accès, l'utilisation et la sécurité des actifs informationnels du Collège Lionel-Groulx. Il oriente les comportements attendus en ce qui a trait à l'utilisation du matériel informatique, des accès et du réseau (intranet et extranet).

Y sont également édictées les règles permettant de préserver les actifs informationnels, la confidentialité, la disponibilité, l'intégrité et la valeur des biens en soutien à la réalisation de la mission du Collège.

3. CADRE LÉGAL, RÈGLEMENTAIRE, ADMINISTRATIF ET NORMATIF

3.1 Cadre légal et règlementaire

Ce Règlement s'inscrit dans un contexte législatif et règlementaire régi par :

- La *Charte des droits et libertés de la personne* (LRQ, chapitre C-12).
- Le Code civil du Québec (LRQ, 1991, chapitre 64).
- La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*.
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03).
- La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1).
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1).
- La Loi sur les archives (LRQ, chapitre A-21.1).
- Le *Code criminel* (LRC, 1985, chapitre C-46).
- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1, r.2).
- La *Directive sur la sécurité de l'information gouvernementale*.
- La *Loi sur les droits d'auteurs* (LRC, 1985, chapitre C-42).
- La *Loi canadienne anti-pourriel* (LRC, 2010, chapitre C-23).

3.2 Cadre administratif

Ce Règlement s'appuie sur :

- La *Politique de la sécurité de l'information du Collège Lionel-Groulx*.
- Le *Règlement sur les conditions de vie du Collège Lionel-Groulx*.

3.3 Cadre normatif

Le présent Règlement s'appuie sur la norme internationale *ISO/CEI 27002 : 2005, Techniques de sécurité : Code de bonnes pratiques pour la gestion de la sécurité de* l'information.

4. CHAMP D'APPLICATION DU RÈGLEMENT

Ce Règlement s'applique, sans exception, à tout utilisateur qui fait usage des ressources et des actifs informationnels du Collège.

Le Règlement énonce les principes qui permettent :

- D'octroyer les accès aux utilisateurs.
- De baliser les accès aux actifs informationnels par les tiers.
- De définir les règles d'utilisation du courrier électronique.
- D'établir un environnement sécuritaire en matière de ressources informationnelles.

5. OBJECTIFS DU RÈGLEMENT

Le Règlement a pour objectif :

- De définir un cadre de référence quant aux bonnes pratiques et aux règles inhérentes à l'utilisation des technologies de l'information.
- De définir les normes applicables en matière de sécurité informatique.
- De prévoir une révision périodique des résultats des vérifications et des contrôles, notamment afin d'y relever les anomalies, les incidents et tout autre élément pertinent.
- De définir les actions à prendre pour corriger les situations anormales ou dangereuses, notamment en ce qui a trait aux processus opérationnels, aux stratégies informatiques et aux achats d'équipement.
- D'informer le comité de direction des travaux, activités, et incidents en matière de sécurité informatique.
- D'assurer le respect des éléments opérationnels requérant l'approbation des différentes directions.

6. DOCUMENTS À L'APPUI DU RÈGLEMENT

Le présent Règlement s'appuie sur la *Politique de la sécurité de l'information* et vient chapeauter les directives en cette matière déjà adoptées par les instances du Collège.

7. ACCÈS AUX TECHNOLOGIES DE L'INFORMATION

L'accessibilité au réseau entraîne une certaine responsabilité pour les utilisateurs. Ceux-ci se doivent en effet de respecter les différents règlements, politiques et directives en vigueur quant à l'accès et à l'utilisation des technologies de l'information mises à leur disposition.

En respect des principes d'imputabilité, la règle générale en ce qui a trait à l'attribution d'un code d'accès est un utilisateur, un code d'accès personnel. Aucun code d'accès générique ne sera émis.

7.1 Code d'accès et mot de passe

a) Tout membre du personnel doit obligatoirement être inscrit aux registres DRH afin d'obtenir un code d'accès aux ressources technologiques du Collège. Ces accès sont octroyés en fonction des tâches inhérentes à chacun des postes.
b) Les accès aux systèmes doivent être maintenus à jour promptement lors des mutations et des départs. La DIIM, conjointement avec la DRH, met en place des mesures de contrôles appropriées pour faciliter la communication lors des arrivées, des départs et des mutations du personnel.
c) Tout étudiant doit être inscrit au Collège pour obtenir un code d'accès aux services technologiques.
d) Les accès aux ressources principales pour les étudiants sont désactivés dès la fin de leurs études au Collège ou, pour ce qui est du personnel, dès la cessation du lien d'emploi ou en cas d'absence prolongée.
e) Les règles prescrites au Collège quant au choix des mots de passe, leur utilisation et leur gestion répondent aux normes de l'industrie.
f) L'utilisateur ne peut, en aucun cas, divulguer ses codes d'accès et ses mots de passe à un autre utilisateur ou à un tiers.
g) Les accès octroyés à un utilisateur peuvent en tout temps être résiliés sans préavis si celui-ci contrevient au cadre légal et règlementaire en vigueur ou qu'il y a menace pour la sécurité du Collège ou d'un tiers.

7.2 Accès distant

La DIIM doit assurer le respect des procédures visant à :

a) Accorder l'accès à distance nécessaire aux utilisateurs ou aux tiers dans le cadre de leurs fonctions.
b) Configurer le réseau afin d'assurer un niveau suffisant de performance et de fiabilité dans le but de répondre aux exigences en matière de sécurité des systèmes.
c) Configurer correctement le matériel et les logiciels d'accès à distance contre les tentatives d'intrusions.
d) Contrôler l'accès à distance par le biais de techniques robustes d'identification.
e) Résilier en tout temps un accès distant, sans préavis, lorsqu'il y a une menace concernant la sécurité du Collège ou d'un tiers.

8. ACCÈS AUX APPLICATIONS

Le code d'accès au réseau du Collège permet l'utilisation des ressources de base, mais ne garantit pas les accès aux applications nécessaires à l'exercice des activités.

Le Collège, dans le respect de la *Politique de la sécurité de l'information*, s'assure que chaque utilisateur ait accès aux ressources informationnelles nécessaires à l'exercice de ses fonctions.

Un registre des propriétaires devra être maintenu à jour et les droits d'accès octroyés aux utilisateurs doivent être autorisés par le propriétaire principal. Le processus d'identification et d'autorisation des accès à une application logicielle est formel, soit par écrit ou via un logiciel utilisé à cette fin. Les accès définis dans le système et dans l'infrastructure sont conformes aux autorisations autorisées par le propriétaire principal de l'application. Une révision périodique des droits d'accès devra être effectuée minimalement tous les trois ans.

9. IMPARTITION ET TIERS

a) Le présent Règlement s'applique autant aux processus impartis qu'aux opérations internes du Collège. Les tiers sont tenus de satisfaire aux exigences de Règlement, aux normes de sécurité, à la documentation technique et aux procédures de sécurité au même titre que le personnel du Collège.
b) Chaque accès par des tiers aux applications logicielles stratégiques est autorisé par la DIIM et est dûment consigné dans un registre administré par celle-ci.

10. UTILISATION DU COURRIER ÉLECTRONIQUE ET D'INTERNET

a) Le courrier électronique et Internet sont strictement utilisés pour les besoins du Collège.
b) L'utilisateur fait usage de mesures de protection et de sécurité adéquates lors de la transmission de documents ou de renseignements de nature confidentielle (protégés en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*). Les mêmes mesures sont prises pour des données à caractère stratégique pour le Collège.
c) Le téléchargement d'information à partir d'Internet et l'ouverture des pièces jointes dans les courriers électroniques doivent être faits avec soin afin d'éviter l'exécution de code malveillant.
d) Dans ses communications avec des personnes physiques ou morales, l'utilisateur doit s'abstenir de tenir des propos injurieux, diffamatoires, haineux ou pouvant constituer une forme de menace, de harcèlement, de dénigrement ou de discrimination.
e) Pour tous courriels diffusés, l'utilisateur s'identifie à titre de signataire du message et précise, s'il y a lieu, à quel titre il s'exprime.
f) Il est interdit d'utiliser un ou des subterfuges ou autres moyens pour transmettre un courrier électronique de manière anonyme ou au nom d'une autre personne.
g) À moins d'avoir obtenu l'autorisation de la part de la DRH, il est interdit d'envoyer des courriers électroniques en chaîne.

11. SÉCURITÉ

La DIIM doit sauvegarder les systèmes électroniques d'information jugés comme étant essentiels à la bonne marche des activités du Collège contre les menaces qui peuvent survenir 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 des services. La DIIM met en place des mesures pour protéger le réseau du Collège contre les menaces informatiques et technologiques.

Ceci exige que la DIIM procède à des contrôles sécuritaires de base permettant d'assurer une surveillance en continu afin d'identifier et d'analyser les menaces et d'établir des mécanismes efficaces face à de telles circonstances .De plus, les utilisateurs sont tenus de rapporter promptement à la DIIM les incidents de sécurité et le non-respect du Règlement par les utilisateurs.

11.1 Menaces externes et internes

L'utilisation des réseaux, y compris le réseau sans fil, est strictement contrôlée afin de prévenir l'usage non autorisé des équipements. La DIIM configure le matériel et les logiciels correctement contre les tentatives d'intrusion.

a) Il est interdit d'utiliser des moyens qui peuvent provoquer des perturbations aux réseaux internes et externes (attaque, piratage, etc.).
b) Tout utilisateur, lorsqu'il accède à un réseau externe, doit se conformer aux règles prescrites de celui-ci.

11.2 Sécurité des installations informatiques

a) La DIIM définit les zones à accès restreint et installe les systèmes de sécurité ainsi que le matériel nécessaire selon une évaluation des menaces et des risques.
b) La DIIM s'assure également de mettre en place les mesures nécessaires afin de protéger les équipements et l'information qu'ils contiennent.

11.3 Sécurité physique de l'espace de travail

a) Il est strictement interdit d'utiliser le matériel informatique à d'autres fins que celles prévues pour les besoins du Collège.
b) La DIIM s'assure du maintien de mesures suffisantes afin de sécuriser les postes de travail laissés sans surveillance.
c) Les utilisateurs doivent prendre des mesures appropriées pour protéger adéquatement les renseignements classifiés et protégés en leur possession.

11.4 Acquisition ou développement de matériels et de logiciels

Tous développements de matériel ou de logiciel ou acquisition doivent obligatoirement être autorisés par la DIIM.

Elle s'assure que :

a) L'acquisition ou le développement de nouveaux produits commerciaux ou maison sont en adéquation avec les orientations du Collège.
b) L'acquisition et le développement de nouveaux produits tiennent compte des exigences en matière de sécurité informatique.
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.

11.5 Copie de sécurité

a) La DIIM met en place des mesures suffisantes afin de protéger l'information numérique du Collège dans des espaces de stockage contrôlé par celui-ci et en respect du cadre législatif et règlementaire en vigueur.
b) La DIIM met en place une procédure de sauvegarde et de recouvrement. Elle effectue des tests en ces matières à intervalle régulier, conserve les copies dans un lieu physique distinct et effectue régulièrement un suivi sur le matériel de sauvegarde.

11.6 Continuité des opérations

Afin d'assurer la prestation continue des services essentiels, la DIIM prépare un plan de continuité opérationnelle de ses activités de recouvrement à la suite d'un incident. Ce plan devra prévoir :

a) Une analyse des impacts afin d'inventorier par ordre de priorité les services et les biens essentiels.
b) Des plans, des mesures et des procédures afin d'assurer la disponibilité en continu des services et des biens essentiels.
c) Des activités de revue, de mise à l'essai et de vérification du plan de continuité.

La DIIM applique un mécanisme de redondance des composantes critiques et effectue un entretien régulier de l'équipement dans le but d'assurer la prestation continue des services essentiels lors d'une panne sans avoir à recourir systématiquement au plan de continuité des opérations.

11.7 Déplacement d'actif informationnel

La DIIM est responsable de maintenir à jour un inventaire de tous les actifs informationnels et de leurs utilisations. Le Collège doit, en tout temps, être en mesure de démontrer la traçabilité d'un actif informationnel.

Dans cette perspective, sans l'autorisation formelle de la DIIM, il est interdit :

a) De déplacer un actif informationnel.
b) De réaffecter un actif informationnel.

c) De changer la vocation d'un actif informationnel.
d) De recueillir des actifs informationnels.

11.8 Disposition des ressources informationnelles

Toute ressource informationnelle, qu'elle soit matérielle ou virtuelle, a un cycle de vie.

Dans cette perspective et conformément à la *Politique de la sécurité de l'information* (chapitre 8) :

a) Seule la DIIM peut disposer du matériel informatique. En ce sens, elle s'assure de mettre en place les mesures appropriées pour effacer complètement le contenu des médias de stockage contenant des renseignements classifiés et protégés ainsi que des logiciels sous licence avant leur disposition finale.
b) 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 organisations.
c) Seul le RSI peut ordonner une destruction massive de données archivées.

11.9 Enquête sur les incidents de sécurité

Le Collège implante des procédures nécessaires relativement aux incidents de sécurité et prend des mesures correctives pour y donner suite.

11.10 Formation et sensibilisation

La DIIM doit :

a) Mettre en place un programme de sensibilisation en matière de sécurité afin d'informer les personnes de leurs responsabilités en matière de sécurité et pour leur faire des rappels périodiques à ces égards.
b) Informer les personnes des privilèges d'accès et des limites reliées à leurs tâches. La DIIM s'assure également de la mise en place de mesures afin d'informer et d'encadrer le personnel quant à l'usage du courrier électronique et d'Internet.

12. CONDITIONS D'UTILISATION SUPPLÉMENTAIRES

L'utilisation des ressources informationnelles du Collège est un privilège et non un droit.

12.1 Droit à la confidentialité

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

a) Dans le cadre d'une menace, la confidentialité de cette information peut être levée si le Collège a des raisons fondées de croire qu'un utilisateur contrevient d'une quelconque façon au cadre législatif et règlementaire en vigueur. Dès lors, le Collège peut procéder à une vérification nominative des renseignements personnels et privés de cet utilisateur.

   Cependant, cette vérification ne peut être conduite sans le consentement de la Direction générale. Une copie de cette autorisation devra être consignée au dossier visé par l'application de cette procédure exceptionnelle.
b) Dans le cadre d'une enquête, un utilisateur peut demander la levée de la confidentialité. Dans ce cas, sauf exception, le Collège devra obtenir le consentement écrit de l'utilisateur concerné avant de procéder à la collecte, à l'utilisation ou à la communication des renseignements personnels. Ce consentement doit être manifeste, libre et éclairé et être donné à des fins spécifiques. De plus, il ne sera valable que pour la durée des opérations de vérification pour lesquelles il a été obtenu.
c) La collecte autorisée est effectuée par la DIIM, un officier du Collège ou une organisation dûment mandatée.

12.2 Utilisation à des fins personnelles

a) Les utilisateurs peuvent faire un usager raisonnable des technologies de l'information à des fins personnelles.
b) Toutes les informations enregistrées par les utilisateurs dans les espaces de stockages du Collège sont accessibles en tout temps par une personne autorisée.
c) Les utilisateurs doivent enregistrer les informations personnelles dans *l'espace personnel* dédié à cette fin.
d) L'utilisation de *l'espace personnel* doit être conforme aux dispositions du présent Règlement.
e) L'utilisation des technologies de l'information à des fins personnelles n'a pas pour effet d'empêcher l'accès aux équipements et aux informations par une personne autorisée autre que l'utilisateur principal lorsque cet accès est requis et qu'il a été autorisé par le supérieur immédiat de celui-ci.

12.3 Utilisation par une personne autorisée

En cas d'absence d'un membre du personnel, l'utilisation de l'ordinateur, de la boîte vocale et des autres ressources informatiques par un autre membre du personnel peut être autorisée.

Cette utilisation doit respecter le principe du moindre accès et n'être octroyée qu'en cas de nécessité. Dans tous les cas où un tel accès est nécessaire, le supérieur immédiat de l'utilisateur absent doit préalablement prendre les moyens raisonnables pour l'en aviser.

13. SANCTIONS

Ce Règlement s'appuie sur le principe que nul n'est censé ignorer la Loi.

Toute contravention au présent Règlement peut mener à la suspension des privilèges d'accès aux ressources informationnelles du Collège. Des mesures administratives, disciplinaires ou légales pourront être entreprises auprès des contrevenants.

14. RESPONSABILITÉS

Chaque direction et service, en collaboration avec la DIIM et le RSI, est responsable de l'application et du respect du présent Règlement.

15. EXAMEN

Le présent Règlement sera réexaminé maximalement tous les cinq ans.

16. ENTRÉE EN VIGUEUR ET ABROGATION

Le présent Règlement a été adopté par le conseil d'administration du 28 novembre 2017 et est entré en vigueur le jour de son adoption.

Le présent Règlement abroge tout autre document ou texte portant sur les mêmes objets adoptés antérieurement.