POLITIQUE RELATIVE AU BON USAGE DES RESSOURCES INFORMATIQUES DE MCGILL

Cette politique remplace :
le *Code de conduite des utilisateurs des installations informatiques de McGill;*
les *Lignes directrices relatives à la gestion des installations informatiques de McGill (McGill Computing Facilities Management Guidelines).*

Préambule

Les ressources de McGill en technologies de l'information (ci-après Ressources TI de McGill) sont destinées à épauler la mission éducative de l'Université et à promouvoir l'avancement du savoir par l'enseignement, la recherche savante et le service à la société. L'Université offre des conditions propices à l'accès au savoir et au partage d'informations. L'Université est chargée de veiller au fonctionnement efficace et fiable de nos systèmes et à la protection de nos ressources en technologies de l'information. La présente politique précise les responsabilités de l'Université et des membres de la communauté universitaire relatives au bon usage des Ressources TI de McGill.

1. Définitions :

Pour l'application de la présente politique :

1.1. « Site web administratif » s'entend des pages ou sites consacrés aux rôles et responsabilité d'une unité au sein de l'Université.

1.2. « Utilisateur autorisé » désigne tout membre de la communauté de l'Université McGill (employé, étudiant, diplômé, administrateur ou toute autre personne) autorisé, dans le cadre de l'exercice de ses fonctions et responsabilités, d'avoir accès à certaines données ou systèmes faisant partie des Ressources TI de McGill.

1.3. « Disponibilité » s'entend de l'accessibilité des Ressources TI de McGill pour les usages auxquels elles sont destinées.

1.4. « Communications radiodiffusées » s'entend des messages électroniques (courriels) ou autres communications électroniques transmises par les Ressources TI de McGill à un groupe, y compris sans toutefois s'y limiter, les listes de diffusion (listservs), listes d'envoi et listes de promotion.

1.5. « CSI » correspond à chef des services d'information.

1.6. « Confidentialité » s'entend de la non-divulgation des coordonnées ou données à des personnes ou systèmes non autorisés.

1.7. « Données confidentielles » s'entend de données à caractère privé, exclusif ou sensible, y compris sans toutefois s'y limiter les données personnelles.

1.8. « Coordonnées » s'entend des identifiants, codes d'accès, numéros de compte, mots de passe, NIP, jetons ou autres authentifications attribués aux utilisateurs autorisés pour avoir accès aux Ressources TI de McGill.

1.9. « Données » s'entend des informations stockées par les Ressources TI de McGill ou transmises par ces dernières, incluant des documents, dossiers, bases de données, courriels et supports multimédias.

1.10. « Intégrité » s'entend de la protection contre toute modification des données par des personnes non autorisées.

1.11. « Lignes directrices des TI » s'entend des lignes directrices ou normes en rapport avec la présente politique figurant dans la base de connaissances des TI ou sur le site des services de TI.

1.12. « Services de TI » s'entend des unités de McGill qui offrent des services de technologies de l'information sur le campus et relèvent du CSI.

1.13. « Adresse électronique de McGill » s'entend d'une adresse électronique émise par les Services des TI à un utilisateur autorisé conformément au format officiel défini par les mêmes services. Par exemple, l'adresse électronique de McGill attribuée aux membres du personnel se présente habituellement sous le format prénom.nom@mcgill.ca et sous le format prénom.nom@mail.mcgill.ca lorsqu'il s'agit des étudiants et diplômés.

1.14. « Ressources TI de McGill » s'entend de toutes les données et de tous logiciels, équipements, systèmes de communications, systèmes de stockage, réseaux et matériels connectés au réseau de l'Université ou faisant usage de ce dernier, quelle que soit la personne chargée de les administrer.

1.15. « Site web thématique public de McGill » s'entend d'un site Web hébergé par les Ressources TI de McGill, accessible à toute personne munie d'un navigateur et ayant accès à Internet.

1.16. « Usage non visé par McGill » s'entend d'un usage non conforme aux dispositions de l'article 2.1.

1.17. « Données personnelles » s'entend d'informations concernant une personne physique qui permettent l'identification de cette personne conformément aux lois relatives à la protection de la vie privée applicables au Canada et au Québec.

1.18. « Sécurité » s'entend de la protection des données et systèmes contre toute infraction ou violation de la disponibilité, de la confidentialité ou de l'intégrité des Ressources TI de McGill.

1.19. « Administrateur de système » s'entend d'une personne chargée, conformément à la description de ses tâches ou des responsabilités qui lui sont imparties, d'établir et d'assurer l'entretien d'un système ou réseau informatique.

1.20. « Réseau de l'Université » s'entend du réseau câblé et radiotéléphonique destiné à la transmission des données, fichiers audio et vidéo placé sous le contrôle des Services des TI.

2. Principes

2.1. Les Ressources TI de McGill appuient la mission de l'Université en matière d'enseignement, de recherche et d'administration.

2.2. Les utilisateurs autorisés doivent utiliser les Ressources TI de McGill de manière éthique, responsable et licite, conformément aux politiques de l'Université.

2.3. Les utilisateurs autorisés sont en droit de s'attendre au respect raisonnable de leur vie privée dans le cadre de l'usage qu'ils font des Ressources TI de McGill.

2.4. Les utilisateurs autorisés doivent prendre toutes les mesures raisonnables pour protéger la confidentialité, l'intégrité et la disponibilité des Ressources TI de McGill.

2.5. Les utilisateurs autorisés ne peuvent avoir accès aux Ressources TI de McGill que conformément aux politiques et procédures de l'Université. La possibilité d'avoir accès aux Ressources TI de McGill n'est pas nécessairement synonyme d'autorisation à le faire.

2.6. Les utilisateurs autorisés doivent respecter la propriété intellectuelle et commerciale, y compris sans toutefois s'y limiter les marques de commerce et les droits d'auteur, des propriétaires de logiciels et de données stockées par les Ressources TI de McGill ou transmises par ces dernières, y compris les ressources des bibliothèques et les archives.

3. Coordonnées

3.1. Les utilisateurs autorisés ne doivent pas partager leurs coordonnées personnelles avec d'autres personnes. Lorsqu'il est impératif qu'un compte soit partagé et que l'application concernée ne permet pas la délégation, l'utilisateur autorisé doit utiliser des coordonnées destinées à cet usage spécifique.

3.2. Les utilisateurs autorisés doivent s'identifier correctement dans les applications, services ou connexions faisant usage des Ressources TI de McGill. Un utilisateur autorisé ne doit pas usurper l'identité d'une autre personne.

3.3. Nonobstant les articles 3.1 et 3.2, les utilisateurs autorisés peuvent rester anonymes lorsque cela est nécessaire ou légitime, comme dans le cas de la participation à certaines enquêtes ou sondages.

4. Sécurité

4.1. Les utilisateurs autorisés doivent prendre toutes les mesures nécessaires pour protéger la sécurité des Ressources TI de McGill et se conformer aux politiques et procédures de l'Université relatives à la protection des données et à la gestion des dossiers.

4.2. Les utilisateurs autorisés ne doivent pas utiliser les Ressources TI de McGill de manière à faire peser un risque de sécurité à l'Université.

4.3. Les utilisateurs autorisés doivent se conformer aux protocoles de l'Université pour signaler les menaces de sécurité et doivent coopérer aux enquêtes diligentées sur d'éventuelles infractions.

4.4. Les personnes qui utilisent les Ressources TI de McGill d'une manière qui constitue une infraction aux politiques et procédures de McGill ou d'une manière qui outrepasse leur autorité s'exposent au risque de voir leurs activités surveillées et enregistrées par les administrateurs de systèmes. Lors de la surveillance des personnes faisant un usage inapproprié des Ressources TI de McGill ou durant les travaux d'entretien ou de mise à niveau des Ressources TI de McGill, les activités des utilisateurs autorisés peuvent éventuellement être surveillées.

5. Données

5.1. Sous réserve de l'article 5.2, l'accès aux données confidentielles est réservé aux utilisateurs autorisés ou aux personnes ayant un besoin légitime d'y avoir accès après avoir été dûment

autorisées à le faire par un utilisateur autorisé. La confidentialité des données consultées doit être préservée et les données ne doivent être utilisées que pour les besoins pour lesquels elles ont été consultées.

5.2. Nonobstant l'article 2.3, l'accès aux données des utilisateurs autorisés peut être accordé à un administrateur désigné de l'Université ayant un intérêt légitime ou étant investi d'une responsabilité à le faire, dans les cas suivants :

(i) Pour assurer la continuité du fonctionnement de l'Université lorsque l'utilisateur autorisé dont les données sont consultées n'est pas disponible ou n'est plus rattaché à McGill.

(ii) Pour enquêter sur les infractions aux politiques ou règlements de l'Université lorsqu'il existe des motifs raisonnables de croire qu'une telle infraction a eu lieu.

(iii) Dans les cas autorisés par la loi.

5.3. Avant de confier le stockage, le traitement ou la transmission de données personnelles à un prestataire de services informatiques sous le contrôle d'une entreprise ou d'un service situé en dehors du Québec, tout utilisateur autorisé doit au préalable consulter le CSI qui consultera lui-même un membre habilité de la haute administration, selon le cas.

6. Courriels et communications radiodiffusées

6.1. Des services de courriel sont offerts aux utilisateurs autorisés pour faciliter le fonctionnement efficace des activités universitaires et administratives.

6.2. Pour s'assurer que les messages électroniques sont gérés conformément à la politique relative à la conservation des données de l'Université, tous les membres du personnel administratif et de soutien doivent s'assurer que leur adresse électronique de McGill dirige les messages électroniques vers un serveur de courrier électronique de McGill. Ceux-ci ne doivent pas configurer leur compte de courrier électronique de McGill de manière à ce que les messages soient redirigés vers une adresse électronique non-McGill sans l'autorisation préalable du CSI ou de son délégué. Les membres du personnel enseignant peuvent rediriger leurs courriels vers un serveur de courrier électronique non-McGill, après s'être assuré que ce serveur bénéficie de protections comparables à celles fournies par l'Université pour les comptes de courrier électronique et qu'il respecte les normes et les lois relatives à la protection de la vie privée, ainsi qu'à la conservation et à la destruction des documents.

6.3. Les utilisateurs autorisés ne doivent transmettre des communications radiodiffusées que si le contenu du message est en rapport avec les fonctions universitaires ou administratives de McGill, et uniquement

(i) si cette personne est autorisée à envoyer un message du fait de ses fonctions, ou

(ii) si le message est envoyé à une liste de diffusion à laquelle les personnes ont adhéré en pleine connaissance de cause.

6.4. Les utilisateurs autorisés rattachés à des unités administratives doivent transmettre leurs communications radiodiffusées conformément aux Lignes directrices des TI relatives aux formats et pièces jointes.

7. Sites web publics

7.1. Un utilisateur autorisé qui publie des informations sur un site web thématique public de McGill doit s'assurer que le contenu se conforme aux politiques et procédures de l'Université.

7.2. Lorsque McGill parraine un site web collaboratif (blogues, wikis ou réseaux sociaux), le site en question doit se conformer aux Lignes directrices des TI.

7.3. Aucune publicité extérieure ou commerciale ne doit apparaître sur un site web public de McGill sans l'autorisation préalable du CSI, lequel doit en référer à un membre habilité de la haute administration. Nonobstant cette disposition, les activités de l'Université, y compris sans toutefois s'y limiter les conférences universitaires, les colloques et autres activités semblables, peuvent être annoncées sur les sites web McGill concernés.

7.4. Les unités de McGill doivent héberger leur site web administratif sur le système d'édition Web de l'Université, sauf si les exigences fonctionnelles des unités universitaires ne peuvent être prises en charge par ledit système d'édition.

7.5. Tous les sites web administratifs doivent être conformes aux Lignes directrices relatives aux publications Web des TI qui précisent les normes Web, les normes de sécurité, les règles d'accessibilité, de même que les règles en matière d'identité visuelle. Les sites web administratifs doivent notamment être correctement identifiés comme étant associés et (ou) appartenant à l'Université McGill et doivent également être configurés de manière à faciliter la navigation d'un site de l'Université à l'autre.

7.6. Les noms de domaine qui incluent le terme « McGill » ne peuvent être ni achetés ni enregistrés par des unités individuelles ou membres du personnel de McGill sans l'approbation du (de la) secrétaire général(e) de l'Université.

8. Réseau

8.1. Les Services des TI ne doivent habituellement pas utiliser de technologies de nature à empêcher un utilisateur autorisé des Ressources TI de McGill à avoir accès à un site web externe lorsque l'ordinateur de ce dernier a été configuré pour avoir accès à Internet.

8.2. Nonobstant l'article 8.1, l'Université peut modérer, filtrer, limiter ou bloquer la circulation sur Internet lorsque celle-ci expose l'Université ou les utilisateurs autorisés à des menaces de sécurité ou lorsque cela est nécessaire pour garantir la confidentialité, l'intégrité ou la disponibilité des Ressources TI de McGill.

8.3. Les utilisateurs autorisés ne doivent pas autoriser l'accès au réseau de l'Université à des membres du public ou à des personnes autres que celles autorisées par les Services des TI, ni en autoriser le partage.

8.4. Les utilisateurs autorisés ne peuvent pas connecter directement au réseau de l'Université des matériels (y compris des commutateurs, routeurs, points d'accès sans fil, réseau privé virtuel et pare-feu) sans l'autorisation préalable des Services des TI. Les exceptions standard précisées dans les Lignes directrices des TI ne nécessitent aucune autorisation préalable.

8.5. Les utilisateurs autorisés ne peuvent connecter directement au réseau de l'Université que des matériels conformes aux Lignes directrices des TI relatives aux logiciels malveillants.

9. Administration des systèmes

9.1. Toutes les Ressources TI de McGill doivent avoir un administrateur de système désigné. Lorsqu'une unité universitaire n'a pas pris de dispositions à cet effet, les chercheurs ou leurs délégués sont les administrateurs des systèmes de recherche qu'ils contrôlent.

9.2. Les administrateurs de systèmes doivent respecter les politiques, procédures et protocoles établis par l'Université et configurer et gérer les systèmes conformément aux bonnes pratiques de l'Université et aux dispositions de la présente politique.

9.3. Dans le cadre de l'exécution de leurs fonctions, les administrateurs de systèmes peuvent surveiller ou accéder systématiquement aux comptes ou utiliser des outils logiciels et matériels (y compris les outils de surveillance ou de contrôle, témoins de connexion, journal d'audit de sécurité et journaux de connexion, copies de sauvegarde et archives) pour suivre ou préserver l'activité du système. Ils ne doivent utiliser ces données que dans le cadre de l'autorité légitime qui leur est impartie et doivent traiter toute donnée consultée à cet effet comme confidentielle.

10. Usages non visés par McGill

10.1. L'Université ne garantit pas le fonctionnement des usages non visés par McGill qui pourraient être faits des Ressources TI de McGill, ni leurs niveaux de confidentialité.

10.2. L'Université McGill se réserve le droit de limiter ou de mettre un terme aux usages non visés par McGill lorsque ceux-ci font peser un risque sur l'Université.

11. Conformité

11.1. Toute infraction aux dispositions de la présente politique peut constituer une infraction disciplinaire et, au besoin, être réglée conformément aux règlements, politiques, codes ou conventions collectives auxquels l'utilisateur autorisé est assujetti.

11.2. Toute personne qui a des motifs raisonnables de croire qu'il y a eu infraction à la présente politique doit signaler ladite infraction au bureau du CSI.

11.3. Un rapport annuel identifiant les types d'accès autorisés par les Services des TI en vertu de la section 5 (Données) doit être préparé par le CSI ou son délégué et remis au vice-principal exécutif. Ce rapport annuel ne doit fournir que des informations groupées et ne doit identifier aucune personne par son nom.

Historique de la présente politique :

Approuvée :		
Sénat	24 mars 2010	Résolution 11B3
Conseil des gouverneurs	12 avril 2010	Résolution 10.1