

| | |
|---|---|
| TITRE DE LA POLITIQUE | POLITIQUE SUR L'UTILISATION RESPONSABLE DES RESSOURCES EN TECHNOLOGIE DE L'INFORMATION DE L'UNIVERSITÉ MCGILL |
| Organisme d'approbation | Conseil des gouverneurs |
| Date d'approbation initiale | 24 mars 2010 – Sénat 12 avril 2010 – Conseil des gouverneurs |
| Date de la dernière mise à jour | 21 mai 2020 – Conseil des gouverneurs |
| Date de la prochaine mise à jour | Mai 2025 |
| Cadre responsable | Vice-principal (administration et finances) |
| Documents connexes | « Documents des TI » accessibles à http://kb.mcgill.ca/ et à https://www.mcgill.ca/it/ |

BUT ET PORTÉE

But

Le but de la *Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill* (la « Politique ») est de veiller à ce que les ressources en technologie de l'information de l'Université McGill (les « Ressources TI de McGill ») soient utilisées pour la réalisation de la mission de l'Université McGill (l'« Université ») et le soutien des activités administratives, financières et de fonctionnement connexes. Pour ce faire, la Politique vise à préserver la sécurité de toutes les Ressources TI de McGill en définissant les responsabilités de l'Université et de la communauté universitaire relativement à l'utilisation de toutes les Ressources TI de McGill.

Portée

La présente Politique régit l'utilisation de toutes les Ressources TI de McGill et s'applique à tous les membres de la communauté universitaire, y compris les enseignants, les employés, les étudiants, les retraités, les diplômés, les personnes nommées, les consultants, les invités et toute autre personne ayant obtenu l'autorisation d'utiliser les Ressources TI de McGill.

CONTENU

1. Définitions

Dans le contexte de la présente Politique, les termes assortis d'une majuscule sont définis comme suit :

- 1.1. « Utilisateur autorisé » désigne un membre de la communauté mcgilloise et comprend les enseignants, les employés, les étudiants, les retraités, les diplômés, les personnes nommées, les

consultants, les invités et toute autre personne ayant obtenu, en raison de son poste et de ses responsabilités, l'autorisation d'accéder à certaines données ou à certains systèmes qui font partie des Ressources TI de McGill.

- 1.2. « Disponibilité » désigne l'assurance d'un accès rapide et fiable aux Ressources TI de McGill pour l'utilisation à laquelle elles sont destinées.
- 1.3. « Communications électroniques » désigne les courriels et tout autre message électronique transmis par l'entremise des Ressources TI de McGill à un groupe d'adresses électroniques, notamment Yammer, les gestionnaires de liste de diffusion, les listes de diffusion et les listes de cours.
- 1.4. « Confidentialité » désigne l'assurance que seuls les Utilisateurs autorisés ou les systèmes autorisés peuvent accéder aux Authentifiants TI ou aux Données.
- 1.5. « Données confidentielles » désigne l'information dont la protection et l'utilisation sont régies par la loi, la réglementation, les exigences du secteur, un contrat ou tout autre règlement, politique ou directive de l'Université McGill en raison de sa nature délicate. Ce terme englobe notamment les Renseignements personnels.
- 1.6. « Données » désigne l'information numérique stockée dans les Ressources TI de McGill ou transmise par ces dernières, ce qui comprend les documents, les fichiers, les bases de données, les courriels et le contenu multimédia.
- 1.7. « Intégrité » désigne l'assurance que les Données sont exactes et cohérentes, et qu'elles ne sont pas modifiées par des utilisateurs non autorisés.
- 1.8. « Authentifiants TI » désigne une preuve d'identité utilisée pour contrôler l'accès aux Ressources TI de McGill, notamment les noms d'utilisateur, les mots de passe, les données biométriques, les certificats numériques et les cartes d'accès.
- 1.9. « Documents des TI » désigne les lignes directrices, les normes et les directives liées à la présente Politique et figurant dans la Base de connaissances des TI ou le site Web des Services des TI.
- 1.10. « Services des TI » désigne l'unité de l'Université McGill qui offre des services de technologie de l'information à la communauté mcgilloise et qui relève du chef des Services d'information.
- 1.11. « Adresse de courriel de McGill » désigne une adresse de courriel créée par les Services des TI pour un Utilisateur autorisé et conforme au modèle officiel des Services des TI.
- 1.12. « Ressources TI de McGill » désigne tous les actifs des TI appartenant à l'Université ou fournis par celle-ci. Cela comprend notamment les Données, les services infonuagiques, les logiciels, le matériel informatique, les systèmes de communication vocale, l'Internet des objets (IdO) et les appareils ainsi que les services qui utilisent ces ressources TI.
- 1.13. « Site Web public de McGill » désigne un site Web hébergé dans les Ressources TI de McGill et

auquel n'importe quel membre du public a accès au moyen d'un navigateur Web et d'une connexion Internet.

- 1.14. « Utilisation non liée à l'Université », également appelée « utilisation personnelle », désigne une utilisation qui ne sert pas à la réalisation de la mission de l'Université ni au soutien des activités administratives, financières et de fonctionnement connexes, ou qui n'a pas été autorisée.
- 1.15. « Renseignements personnels » désigne les renseignements qui concernent une personne physique et permettent de l'identifier, au sens des lois relatives à la protection de la vie privée applicables.
- 1.16. « Sécurité » désigne la protection de la Confidentialité, de l'Intégrité et de la Disponibilité des Ressources TI de McGill.
- 1.17. « Administrateur de système » désigne une personne responsable, en raison de la description de son poste ou des responsabilités rattachées à son poste, de la mise en place et de la maintenance d'un système ou d'un réseau informatique.
- 1.18. « Réseau de l'Université » désigne le réseau filaire et sans fil géré par les Services des TI et permettant la transmission de Données, de la voix et de vidéos.

2. Principes

- 2.1. Les Ressources TI de McGill sont fournies uniquement aux Utilisateurs autorisés aux fins de réalisation de la mission de l'Université et de soutien des activités administratives, financières et de fonctionnement connexes.
- 2.2. Les Utilisateurs autorisés doivent utiliser les Ressources TI de McGill aux fins indiquées au paragraphe 2.1, d'une manière responsable, éthique et licite, conformément aux politiques, aux directives et aux procédures de l'Université et à d'autres normes et lignes directrices pertinentes de l'Université, et dans le respect des lois et des règlements applicables ainsi que, dans certaines circonstances, des contrats et des ententes de l'Université.
- 2.3. Les Utilisateurs autorisés peuvent raisonnablement s'attendre à ce que leur vie privée soit respectée lorsqu'ils utilisent les Ressources TI de McGill.
- 2.4. Les Utilisateurs autorisés doivent prendre des mesures raisonnables et prudentes afin de préserver la Sécurité et d'assurer la Confidentialité, l'Intégrité et la Disponibilité des Ressources TI de McGill.
- 2.5. La capacité d'accéder aux Ressources TI de McGill et de les utiliser ne constitue pas une autorisation de le faire.
- 2.6. Les Utilisateurs autorisés doivent respecter les droits de propriété intellectuelle d'autrui.
- 2.7. Les Utilisateurs autorisés doivent utiliser la technologie conformément aux Documents des TI et

aux pratiques exemplaires de l'Université.

3. Authentifiants TI

- 3.1. Les Utilisateurs autorisés ne doivent pas divulguer leurs Authentifiants TI personnels.
- 3.2. S'il est essentiel qu'un Authentifiant TI soit divulgué et que l'application n'offre pas l'accès délégué, l'Utilisateur autorisé doit avoir recours à un Authentifiant TI ad hoc, par exemple grâce à l'utilisation d'un compte de ressources ou d'une boîte aux lettres partagée.
- 3.3. Lorsqu'ils utilisent les Ressources TI de McGill, les Utilisateurs autorisés doivent établir leur identité correctement à l'aide de leurs Authentifiants TI pour ouvrir des applications, se prévaloir de services ou ouvrir des sessions. Un Utilisateur autorisé ne doit pas se faire passer pour une autre personne, sauf s'il en a obtenu explicitement la permission pour certaines applications dans le but de procéder à des tests ou à une configuration.
- 3.4. Nonobstant le paragraphe 3.3, les Utilisateurs autorisés peuvent conserver l'anonymat pour des raisons légitimes, par exemple pour répondre à certains sondages.

4. Sécurité

- 4.1. Les Utilisateurs autorisés ne doivent pas utiliser les Ressources TI de McGill d'une manière susceptible de compromettre la Sécurité de ces dernières ou d'exposer l'Université à des risques.
- 4.2. Les Utilisateurs autorisés doivent signaler les menaces réelles ou potentielles pour la Sécurité des Ressources TI de McGill dont ils soupçonnent l'existence, conformément aux directives et aux protocoles pertinents des TI, et collaborer aux enquêtes sur de possibles failles.
- 4.3. Les Utilisateurs autorisés ne doivent pas tenter de contourner les mesures de contrôle de la sécurité des TI sans l'autorisation écrite préalable des Services de sécurité des TI.

5. Données

- 5.1. Sous réserve des dispositions du paragraphe 5.2, seuls les Utilisateurs autorisés ou des personnes ayant obtenu le consentement d'un Utilisateur autorisé ou s'étant vu accorder, à des fins légitimes, un droit d'accès par un Utilisateur autorisé peuvent accéder aux Données confidentielles. La Confidentialité des Données consultées doit être protégée et les Données doivent être utilisées uniquement aux fins pour lesquelles elles ont été consultées.
- 5.2. Nonobstant le paragraphe 2.3, l'accès aux Données d'un Utilisateur autorisé peut être accordé à un administrateur désigné de l'Université qui, en l'occurrence, a un intérêt et des responsabilités légitimes, dans les cas suivants :
 - i) pour assurer le maintien des activités de l'Université, lorsqu'on doit accéder aux Données d'un Utilisateur autorisé qui n'est pas disponible ou ne travaille plus à

l'Université McGill;

- ii) pour enquêter sur une violation des politiques ou des règlements de l'Université s'il existe des motifs raisonnables de croire qu'il y a eu pareille violation;
- iii) lorsque la loi le permet.

5.3. Lorsqu'un Utilisateur autorisé envisage d'avoir recours aux services d'un fournisseur de technologies de l'information pour le stockage, le traitement ou la transmission de Données institutionnelles, il doit consulter le Service des approvisionnements dès le début du processus. Au besoin, le Service des approvisionnements consultera les Services des TI et les Services juridiques.

6. Courriels et communications électroniques

6.1. Les courriels doivent être conformes aux normes et aux lois régissant la vie privée ainsi que la conservation et la destruction des documents. Par conséquent, les Utilisateurs autorisés membres du corps professoral et du personnel doivent obtenir l'autorisation du chef des Services d'information, ou de son représentant, pour :

- i) transférer ou rediriger systématiquement ou automatiquement leurs courriels vers un serveur de courriel externe; ou
- ii) configurer le téléchargement ou l'extraction de tous leurs courriels vers un serveur de courriel externe.

Il est permis de transférer ou de rediriger manuellement certains courriels, sous réserve d'autres dispositions des politiques et des règlements de l'Université McGill.

6.2. Les Utilisateurs autorisés ont le droit d'envoyer des Communications électroniques si le contenu du message est lié aux fonctions d'enseignement, de recherche et d'administration de l'Université McGill et si :

- i) l'Utilisateur autorisé a le droit d'envoyer le message du fait de ses fonctions; ou
- ii) l'Utilisateur autorisé a le droit d'envoyer le message aux personnes qui se sont abonnées sciemment aux envois en question.

6.3. Les Utilisateurs autorisés qui font partie d'unités administratives doivent envoyer les Communications électroniques conformément aux dispositions des Documents des TI en matière de Sécurité, plus précisément en ce qui a trait aux pratiques exemplaires, aux formats et aux pièces jointes.

7. Sites Web publics

7.1. L'Utilisateur autorisé qui publie de l'information sur un Site Web public de McGill doit s'assurer que le contenu n'enfreint pas la présente Politique, une autre politique, directive ou procédure de l'Université ou une loi ou un règlement applicable.

- 7.2. Aucune publicité externe ou commerciale ne doit apparaître dans un Site Web public de McGill sans l'autorisation écrite préalable de l'unité Communications et relations externes, qui consultera, au besoin, le cadre supérieur approprié. Nonobstant cette disposition, les commandites d'activités de l'Université, notamment des conférences universitaires et des symposiums, peuvent être mentionnées dans les sites Web appropriés de McGill.
- 7.3. Tous les sites Web de McGill doivent être créés conformément au cadre de gouvernance des communications numériques de McGill, qui définit les normes Web et les normes de sécurité, les conventions d'appellation, l'accessibilité, l'identité visuelle et l'image de marque.
- 7.4. Les noms de domaine qui contiennent le mot « McGill » ne doivent pas être achetés ni enregistrés par une unité ou un employé de l'Université sans l'autorisation de l'unité Communications et relations externes.
- 7.5. L'analytique Web et le pistage des utilisateurs soulèvent des questions relevant de l'éthique et de la protection de la vie privée. Les Données recueillies à ces fins se limitent aux interactions avec les liens, les boutons et les éléments des pages. La collecte de Renseignements personnels et de Données confidentielles doit se faire conformément aux lois applicables.

8. Réseau

- 8.1. L'Université peut limiter ou bloquer le trafic Internet lorsque ce dernier compromet la Sécurité de l'Université ou des Utilisateurs autorisés, ou lorsqu'une telle mesure est nécessaire pour assurer la Confidentialité, l'Intégrité ou la Disponibilité des Ressources TI de McGill.
- 8.2. Les Utilisateurs autorisés ne doivent pas donner accès au Réseau de l'Université au public ou à d'autres personnes, ou partager le réseau avec eux, sans avoir obtenu préalablement l'autorisation écrite des Services des TI.
- 8.3. Les Utilisateurs autorisés ne doivent pas connecter de dispositifs de réseau (notamment les commutateurs, les routeurs, les points d'accès sans fil, les réseaux privés virtuels et les pare-feu) au Réseau de l'Université sans avoir obtenu préalablement l'autorisation écrite des Services des TI. Dans le cas des exceptions normales décrites dans les Documents des TI, aucune autorisation supplémentaire n'est requise.
- 8.4. Les Utilisateurs autorisés ne peuvent connecter au Réseau de l'Université que des dispositifs conformes aux critères des Documents des TI sur la cybersécurité.

9. Administration des systèmes

- 9.1. Un Administrateur de système doit être dûment affecté à chacune des Ressources TI de McGill. Si une unité universitaire n'a pas pris d'autres dispositions, les chercheurs, ou leurs représentants, sont les Administrateurs des systèmes de recherche dont ils sont responsables.
- 9.2. Les Administrateurs de système doivent respecter les politiques, les directives, les normes et les procédures établies par l'Université, et configurer et gérer les systèmes conformément aux

pratiques exemplaires de l'Université.

- 9.3. Nonobstant le respect de la vie privée des utilisateurs, les Administrateurs de système peuvent surveiller des comptes ou y accéder régulièrement, ou utiliser des outils logiciels et matériels (notamment des outils de surveillance ou de contrôle, des témoins, des pistes et des listes de vérification, des sauvegardes et des archives), à des fins de suivi ou de préservation de l'activité dans le système. Les Administrateurs de système ne peuvent utiliser ces Données que dans les limites de leur autorité légitime et doivent les traiter comme de l'information confidentielle.
- 9.4. Les Administrateurs de système pourraient surveiller ou enregistrer les activités des Utilisateurs autorisés qui, lors de l'utilisation des Ressources TI de McGill, enfreignent les politiques et les procédures de l'Université ou dépassent les limites de leur autorité. Les activités des Utilisateurs autorisés pourraient également être surveillées lors de l'observation de personnes qui font un usage inapproprié des Ressources TI de McGill ou dans le cadre de travaux de maintenance des Ressources TI de McGill.

10. Utilisation non liée à l'Université

- 10.1. L'Université ne garantit aucun service ni niveau de Confidentialité pour l'Utilisation non liée à l'Université des Ressources TI de McGill.
- 10.2. L'Université McGill se réserve le droit de limiter une Utilisation non liée à l'Université, ou d'y mettre fin, si cet usage l'expose à des risques.

11. Mise en application

- 11.1. La violation des dispositions de la présente Politique peut constituer une infraction disciplinaire et, s'il y a lieu, être traitée en fonction des règlements, des politiques, des codes ou des conventions collectives régissant l'Utilisateur autorisé.
- 11.2. Toute personne qui a des motifs raisonnables de croire que la présente Politique a été enfreinte doit signaler la situation au chef des Services d'information.
- 11.3. Les chefs d'unités, ou leurs représentants, doivent rédiger un rapport décrivant le type d'accès accordé en vertu du paragraphe 5.2 (Données) et remettre ce rapport au chef des Services d'information sur demande. Le chef des Services d'information doit ensuite rendre compte de cette activité au vice-principal (administration et finances). Le rapport doit contenir des données agrégées, et le nom des personnes ne doit pas y être mentionné.

APPROBATION DES PROCÉDURES

Le vice-principal (administration et finances), ou son représentant, a le pouvoir de définir et de modifier les procédures nécessaires à l'application de la présente Politique.

RÉVISION

La version révisée de la présente Politique entre en vigueur le 21 mai 2020.

La présente Politique sera révisée tous les cinq ans après la date de sa dernière mise à jour.