Directive relative aux services d'infonuagique

Publiée par : Dirigeant principal de l'information et directeur et responsable de l'application des règles contractuelles, Services d'approvisionnement
Date de révision : 26 mai 2021
Date d'entrée en vigueur : 30 mars 2015

Préambule

La présente directive s'applique à tous les membres de la communauté mcgilloise qui font l'acquisition ou l'utilisation de services d'infonuagique touchant les données opérationnelles ou les données de recherche.

Les objectifs de la directive s'énoncent comme suit :

- Veiller à protéger les renseignements personnels, les renseignements personnels sur la santé, les renseignements exclusifs et la propriété intellectuelle.
- Veiller au respect de la loi par l'Université McGill (comme la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels), les règlements et les normes (comme la norme de sécurité des données de l'industrie des cartes de paiement).
- Compléter et confirmer les autres politiques, directives, procédures et normes de McGill, dont les suivantes :
  - Politique d'approvisionnement
  - Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill
  - Règlement relatif à la conduite de la recherche
  - Politique relative à l'approbation des contrats et à la désignation des signataires autorisé(e)s
  - Policy on Enterprise Data Governance (Politique sur la gouvernance des données opérationnelles)
  - Standard on Enterprise Data Governance (Norme sur la gouvernance des données opérationnelles)
  - Standard on Enterprise Data Classification (Norme sur la classification des données opérationnelles)
  - Secure Use of McGill Administrative Systems Directive (Directive sur l'utilisation sécurisée des systèmes administratifs de McGill)

1. Termes employés et définitions

Aux fins de la présente directive, les termes suivants revêtent le sens qui leur est attribué ci-dessous. Tout terme qui n'est pas défini dans la présente politique revêt le sens qui lui est attribué dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill.

1.1. « **Utilisateur autorisé** » a le sens qui lui est attribué dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill.
1.2. « **Nuage informatique** » désigne l'Internet.
1.3. « **Service d'infonuagique** » désigne un service qui est fourni à la demande sur l'Internet. Ce service permet d'accéder à des applications et à des ressources sans avoir besoin d'infrastructure ou de matériel interne.
1.4. « **Services d'infonuagique pour les données opérationnelles** » désigne les ressources ou services dans le nuage informatique qui ont été approuvés par McGill par rapport à une classe de données en particulier, et pour lesquels le service d'infonuagique a été évalué par les services d'approvisionnement et de technologie de l'information, en collaboration avec les services juridiques au besoin.
1.5. « **Services d'infonuagique pour les données publiques externes** » englobe les données opérationnelles publiques et les données de recherche publiques.
1.6. « **Services d'infonuagique pour les données de recherche** » désigne les ressources ou services qui sont directement accessibles par les chercheurs dans le nuage informatique afin de leur permettre de mener des recherches. Précisons que ces services ne comprennent pas les activités administratives effectuées pour appuyer la recherche.
1.7. « **Données confidentielles** » a le sens qui lui est attribué dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill. Cela comprend les **données opérationnelles réglementées**, les **données opérationnelles protégées**, les **données de recherche réglementées** et les **données de recherche protégées**.

1.8. « **Classification des données** » désigne les trois classes de données suivantes : réglementées, protégées ou publiques.
1.9. « **Dépositaire des données** » a le sens qui lui est attribué dans la Politique sur la gouvernance des données opérationnelles (Policy on Enterprise Data Governance). Les chercheurs sont, par défaut, les dépositaires de leurs données de recherche, sauf s'il en est décidé autrement par un dépositaire des données désigné par la politique.
1.10. « **Données opérationnelles** » a le sens qui lui est attribué dans la Norme sur la classification des données opérationnelles (Standard of Enterprise Data Classification).
1.11. « **Appareil appartenant à l'établissement ou géré par lui** » a le sens qui lui est attribué dans la Directive sur l'utilisation sécuritaire des systèmes administratifs de McGill (Secure Use of McGill Administrative Systems Directive).
1.12. « **Authentifiants TI** » a le sens qui lui est attribué dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill.
1.13. « **Services des TI** » a le sens qui lui est attribué dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill.
1.14. « **Ressources TI de McGill** » a le sens qui lui est attribué dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill.
1.15. « **PCI** » désigne l'industrie des cartes de paiement. Celle-ci regroupe les organisations de commerçants qui stockent, traitent et transmettent les données des titulaires de cartes de paiement (comme les cartes de crédit).
1.16. « **Renseignements personnels** » a le sens qui lui est attribué dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill (par exemple, tout élément des dossiers d'étudiants, des dossiers d'employés, des dossiers de patients, des renseignements sur les donateurs et des renseignements personnels sur la santé).
1.17. « **Renseignements personnels sur la santé** » désigne les informations personnelles relatives à la santé d'une personne (comme les dossiers médicaux et pharmaceutiques).
1.18. « **Données opérationnelles protégées** » a le sens qui lui est attribué dans la Norme sur la classification des données opérationnelles (Standard on Enterprise Data Classification).
1.19. « **Données de recherche protégées** » désigne les données de recherche dont la protection et l'utilisation sont régies par un contrat ou par un règlement, une politique ou une directive de McGill en raison de leur nature confidentielle.
1.20. « **Données opérationnelles publiques** » a le sens qui lui est attribué dans la Norme sur la classification des données opérationnelles (Standard on Enterprise Data Classification).
1.21. « **Données de recherche publiques** » désigne les données de recherche qui sont considérées comme accessibles au public et qui ne sont pas confidentielles.
1.22. « **Données opérationnelles réglementées** » a le sens qui lui est attribué dans la Norme sur la classification des données d'entreprise (Standard on Enterprise Data Classification), comme les renseignements personnels, les renseignements personnels sur la santé et les données relatives aux cartes de paiement.
1.23. « **Données de recherche réglementées** » désigne les données de recherche dont la protection et l'utilisation sont imposées par la loi ou un règlement, comme les renseignements personnels ou les renseignements personnels sur la santé.
1.24. « **Données de recherche** » a le sens qui lui est attribué dans la Politique sur la gouvernance des données opérationnelles (Policy on Enterprise Data Governance). Aux fins de la présente directive, les données de recherche excluent particulièrement les données de cartes de paiement.
1.25. « **Chercheur** » a le sens qui lui est attribué dans le Règlement sur la conduite de la recherche.

2. Principes

2.1. Les données pouvant comporter différents degrés de sensibilité, il faut prévoir différents niveaux de sécurité et de protection des données. Certaines données peuvent être stockées dans le nuage informatique, mais non pas diffusées ou synchronisées avec des appareils.
2.2. Certains renseignements personnels sont toujours considérés comme sensibles (comme les renseignements sur la santé ou la rémunération), mais tout renseignement personnel peut être considéré comme plus sensible en fonction du contexte. Le degré de protection requis par le service d'infonuagique est déterminé par le règlement applicable, la sensibilité des renseignements personnels, les fins pour lesquelles ils doivent être utilisés, leur nombre, leur distribution et le support sur lequel ils sont stockés.
2.3. Tous les services d'infonuagique et fournisseurs de services d'infonuagique ne font pas preuve de la même diligence en matière de cybersécurité et de pratiques de protection de la confidentialité. Une diligence raisonnable et une évaluation des risques sont nécessaires dès lors que des **données confidentielles** sont en jeu. Des risques importants en matière de sécurité et de confidentialité se posent dès lors qu'on offre des services aux consommateurs.
2.4. Les lois sur la protection de la vie privée applicables au Québec imposent à l'Université McGill et à ses fournisseurs

de services d'infonuagique des obligations qui sont sensiblement différentes de celles imposées aux particuliers et même aux entreprises privées. Tous les contrats dans le cadre desquels des renseignements personnels peuvent être hébergés par ou rendus accessibles à un fournisseur de services d'infonuagique et ses sous-traitants doivent respecter les exigences contractuelles établies dans les lois québécoises sur la protection des renseignements personnels pour les organismes publics.

2.5. Les politiques de l'Université exigent la conservation des informations pour des raisons opérationnelles et de conformité réglementaire. L'une de ces obligations est le devoir de savoir quelles données sont stockées, dans quel lieu, et sous quelle forme (p. ex., copies de sauvegarde). Les services d'infonuagique ne fournissent pas tous des mesures adéquates de sauvegarde. Par conséquent, ils ne doivent pas servir à héberger des originaux uniques de données opérationnelles et de recherche.

2.6. L'utilisation des **données confidentielles** doit respecter des principes de sécurité qui comprennent, sans s'y limiter :

2.6.1. Le principe du « moindre privilège », c'est-à-dire les échanges fondés sur le besoin, en n'accordant que les privilèges minimums requis pour effectuer la tâche, et ce, pendant la durée de celle-ci. Les **données confidentielles** ne doivent être transmises qu'à des utilisateurs autorisés ayant un besoin légitime d'y avoir accès compte tenu de leur rôle et de leur niveau de responsabilité. La confidentialité des données consultées doit être préservée, et les données ne doivent être utilisées qu'aux fins pour lesquelles l'accès a été prévu.

2.7. Les utilisateurs autorisés doivent se conformer aux obligations de confidentialité énoncées dans la Politique sur l'utilisation responsable des ressources en technologie de l'information de l'Université McGill.

2.8. Les utilisateurs autorisés sont chargés de déterminer la classe à laquelle leurs données appartiennent et d'assumer les conséquences d'une détermination incorrecte de leur part. En cas de doute, les utilisateurs autorisés doivent se conformer aux conseils des services de TI, des services d'approvisionnement et des services juridiques pour déterminer la classe à laquelle leurs données appartiennent.

2.9. Le stockage des authentifiants TI est un cas spécifique de stockage de données, car il permet d'accéder à d'autres données qui peuvent appartenir à une autre classe de données, notamment des données réglementées. Le niveau de protection requis pour les authentifiants TI doit correspondre au niveau de protection requis par la classe de données auxquelles ils donnent accès. Nonobstant ce qui précède, les authentifiants TI qui permettent d'accéder aux **données opérationnelles réglementées** et aux **données de recherche réglementées** ne doivent pas être stockés dans le nuage informatique, sauf si la solution a été évaluée par les services des TI, en consultation avec les services juridiques au besoin.

3. Acquisition de services d'infonuagique (p. ex., comptes de service, contrats)

3.1. Avant l'acquisition, une approbation écrite est requise de la part du dépositaire des données relativement au caractère approprié de l'utilisation du nuage informatique pour stocker, traiter ou transmettre des **données confidentielles**.

3.2. Si vous faites l'acquisition d'un service d'infonuagique pour stocker, traiter ou manipuler des données (et ce, même si la solution est gratuite), le fournisseur de ce service devient un fournisseur de l'Université. Si le fournisseur manipule des renseignements personnels, il faut intégrer au contrat la version la plus récente de l'annexe sur la protection des renseignements personnels de McGill.

3.3. Les **services d'infonuagique pour les données opérationnelles** sont évalués et approuvés conjointement par les services d'approvisionnement et les services des TI, en collaboration avec les services juridiques au besoin, conformément au processus d'acquisition des services d'infonuagique. Cette approbation comprend une diligence raisonnable, y compris la réalisation d'une évaluation de la protection de la vie privée, une évaluation informatique par les services des TI, la mise en œuvre de mesures de protection et une évaluation du contrat. L'approbation suppose une surveillance continue par l'unité responsable et le respect par les utilisateurs autorisés des mesures de protection mises en place.

3.4. Les **services d'infonuagique pour les données de recherche** sont évalués par le chercheur en vue de leur utilisation conformément au comité d'éthique de la recherche de McGill. Le fournisseur de services d'infonuagique doit être sélectionné conformément à la Politique d'approvisionnement, et le contrat doit être signé et examiné conformément à la Politique relative à l'approbation des contrats et à la désignation des signataires autorisé(e)s. Les **services d'infonuagique pour les données de recherche** peuvent héberger ou consulter des données de recherche uniquement. Les chercheurs doivent effectuer une diligence raisonnable, notamment en procédant à une évaluation des risques et en mettant en place des mesures de protection. Les preuves de la diligence raisonnable exercée par le chercheur doivent être conservées pendant toute la durée du contrat avec le fournisseur de services d'infonuagique et pendant trois ans par la suite. Les utilisateurs autorisés doivent consulter le dirigeant principal de l'information ou son mandataire pour obtenir des conseils sur la diligence raisonnable.

Tableau 1. Partie responsable de la diligence raisonnable pour l'acquisition des services d'infonuagique

Données	**Diligence raisonnable[1]**	
	Évaluation de la confidentialité	**Évaluation des TI et du contrat**
Services d'infonuagique – données opérationnelles	Services d'approvisionnement, juridiques et des TI	
Services d'infonuagique – données de recherche	Comité d'éthique de la recherche[2]	Chercheur
Services d'infonuagique – données publiques externes	Aucune diligence raisonnable exigée	

1 L'évaluation de la solution nécessite une diligence raisonnable par l'entremise d'évaluations de la confidentialité, des TI et du contrat.

2 Comité d'éthique de la recherche (CER), Comité d'éthique et de conformité de la recherche (CEI)

3.5. Les services des TI aideront les demandeurs, à leur demande, durant le processus d'acquisition de services d'infonuagique.

3.6. Les **données confidentielles** doivent toujours être soumises au processus d'acquisition des services d'infonuagique.

3.7. Si un fournisseur de services fait appel à un service d'infonuagique dans le cadre de ses activités, le fournisseur de ce service d'infonuagique devient son sous-traitant. Le recours à des sous-traitants doit être un sujet abordé dans le contrat du fournisseur (y compris la conformité juridique, les exigences en matière de cybersécurité, l'attribution de la responsabilité civile, la responsabilité et les coûts liés aux actions des sous-traitants ou de leurs produits).

3.8. L'utilisation d'un bon de commande de l'Université McGill est obligatoire pour l'acquisition de services d'infonuagique. En particulier, le paiement au moyen de la carte d'achat ou d'une carte de crédit personnelle (et le remboursement ultérieur par l'Université McGill) n'est pas autorisé sans l'autorisation écrite du service d'approvisionnement.

4. Utilisation des services d'infonuagique

4.1. Lorsque des **données opérationnelles réglementées** ou des **données opérationnelles protégées** sont stockées dans un service d'infonuagique, elles ne peuvent être synchronisées qu'avec un appareil appartenant à l'Université ou géré par elle (téléphones mobiles, ordinateurs portables, ordinateurs de bureau), et seulement si le canal de communication est crypté et si cet appareil est protégé par un mot de passe ou authentifiant TI. Si l'application de synchronisation ne stocke pas de copie locale sur l'appareil mais fournit uniquement un accès aux données lorsqu'elle est connectée, cette restriction (appareil appartenant à l'Université ou géré par lui) ne s'applique pas tant que le canal de communication est crypté et que l'appareil est protégé par un mot de passe ou authentifiant TI.

4.2. Vous êtes responsable d'utiliser les services d'infonuagique uniquement aux fins prévues et approuvées. Le service d'approvisionnement doit décrire par écrit l'utilisation approuvée de tous les **services d'infonuagique pour les données opérationnelles**. Il vous incombe de consulter les services des TI et d'approvisionnement avant de modifier l'utilisation d'un tel service d'infonuagique. Si vous contournez les mesures de protection et les capacités de surveillance mises en place par le service des TI ou à sa demande, ou si vous autorisez sciemment un tel contournement, votre unité responsable et vous-même à titre individuel êtes responsables de toute fuite de données et de toute violation de la sécurité touchant ces données.

4.3. Même si la présente directive autorise le stockage de **données opérationnelles réglementées** ou de **données**

opérationnelles protégées dans un service d'infonuagique en particulier, il faut démontrer un besoin professionnel valide, conforme à la portée présentée et approuvée par les dépositaires des données, avant de pouvoir communiquer des données (comme celles sur les ressources humaines) à l'interne ou à l'externe. Cette disposition vise à contrôler le nombre de systèmes hébergeant des données sensibles afin de limiter l'exposition aux risques de cybersécurité.

5. Application des mesures et conformité

5.1. Toutes les données qui ont été hébergées dans des services d'infonuagique qui sont en violation de la présente directive doivent être relocalisées rapidement vers un service conforme, ou l'utilisation du service non conforme doit cesser. Une fois la relocalisation effectuée, l'unité responsable doit veiller à supprimer les données des services d'infonuagique non conformes.

5.2. Toute violation de la présente directive peut mener à une mesure disciplinaire et, le cas échéant, sera traitée selon les règlements, politiques, code ou convention collective à laquelle l'utilisateur autorisé est assujetti.

5.3. Si vous acquérez ou utilisez un service d'infonuagique en contournant le processus d'acquisition des services d'infonuagique, votre unité responsable et vous-même à titre individuel êtes responsables de toute fuite de données et de toute violation de la sécurité touchant ces données. Dans certains cas, les conséquences comprennent des amendes, la responsabilité financière à l'égard de la notification de la fuite de données et toute autre mesure visant à réparer les dommages. L'unité responsable et vous-même à titre individuel risquez de vous voir retirer l'accès à ce service d'infonuagique et d'avoir à payer les coûts afférents en plus des coûts de migration des données vers un service d'infonuagique conforme aux exigences de McGill.

5.4. Toute personne ayant des motifs raisonnables de croire qu'il y a eu une violation de la présente directive doit signaler le problème au bureau du dirigeant principal de l'information. Les signalements anonymes, tels que ceux prévus par la Politique sur la divulgation d'actes répréhensibles, sont acceptés, mais il faut fournir suffisamment de détails pour permettre une enquête adéquate sur le problème tout en minimisant les perturbations causées par cette enquête.

5.5. Si les données tombent dans plus d'une catégorie selon la classification des données, le niveau de protection requis pour ces données est celui qui correspond au niveau de protection le plus élevé.

5.6. Les services des TI peuvent vérifier de temps à autre si les utilisateurs autorisés et des unités responsables respectent la présente directive.

6. Révision

6.1. La présente directive est un document évolutif qui sera mis à jour selon l'évolution des risques de sécurité et de confidentialité.