



**Ministère de la Santé
et des Services sociaux**

Direction générale des technologies de l'information

Sécurité de l'information

Outils de collaboration

Termes et conditions d'utilisation des outils de collaboration

Version : 0.13

Approuvé par : Luc Bouchard, sous-ministre associé et dirigeant réseau de l'information

Mise à jour du document: 2020-03-16

Note importante à l'intention du lecteur

Dans les circonstances de la pandémie du COVID-19 qui sévit et l'état d'urgence sanitaire que le gouvernement du Québec a décrété, la mise en œuvre des outils de collaboration a été accélérée. Cependant, le projet est encore en phase pilote, certaines activités de préparation de l'environnement n'ont pu être menées à terme. En conséquence, bien qu'autorisé par le présent document, vous devez restreindre vos communications confidentielles, de recherche, ainsi que celles à caractère clinique, social ou personnel via cette plateforme aux situations extrêmes qui l'exigent. Cette restriction sera levée aussitôt que la mise en place et la configuration de l'environnement seront complétées.

Également, le présent document est appelé à évoluer, nous vous en informerons le moment venu.

1. Préambule

Dans le cadre des orientations gouvernementales visant une utilisation efficace et efficiente des technologies de l'information, le ministère de la Santé et des Services sociaux (MSSS) offre à ses utilisateurs¹, ainsi qu'aux utilisateurs des établissements et organismes du réseau de la santé et des services sociaux (RSSS), une panoplie d'outils de collaboration à usage professionnel, permettant ainsi d'accroître leur capacité de collaboration.

Les outils de collaboration acquis par le MSSS se déclinent comme suit :

- Outlook : Système de messagerie, calendrier, planificateur de tâches, etc.;
- OneDrive Entreprise : Stockage des fichiers professionnels et personnels;
- SharePoint Online : Partage et gestion de contenu;
- Microsoft Teams : Échange instantané d'informations, de fichiers, etc.;
- Microsoft Forms : Enquêtes et sondages;
- Sway : Création et partage des rapports, présentations, récits personnels interactifs;
- Power Automate : Création de flux de travaux entre les applications, les fichiers et les données;
- Office 365 MyAnalytics : Analyse des données pour une meilleure productivité;
- Microsoft Planner : Gestionnaire de projet;
- Microsoft Stream : Partage de vidéo, de présentations et de réunion.

2. Objectifs

Le présent document a pour objectif d'encadrer l'utilisation des outils de collaboration. Il énonce à cet égard des règles d'utilisation, au regard de la sécurité de l'information, permettant ainsi de maintenir le niveau de sécurité global adéquat pour le MSSS et le RSSS, tout en exploitant pleinement les capacités et les fonctionnalités des outils de collaboration.

3. Termes et conditions d'utilisation des outils de collaboration

Les outils de collaboration offerts par le MSSS répondent aux exigences ministérielles et gouvernementales de sécurité de l'information. Les utilisateurs sont tenus donc d'utiliser, dans le cadre de leurs fonctions, les outils de collaboration fournis par le MSSS et d'en adopter un usage exemplaire, au regard des dispositions du cadre de gouvernance de la sécurité de l'information et des meilleures pratiques en la matière.

¹ L'utilisateur est défini comme étant une personne physique ou morale, ou un système à qui un accès aux outils de collaboration a été accordé et qui l'utilise dans le strict cadre de ses fonctions.

3.1 Termes et conditions générales

Les outils de collaboration ne doivent aucunement se substituer aux processus d'affaires en place, ils viennent compléter l'offre de service ministérielle en matière de technologie de l'information.

3.1.1 Règles relatives aux échanges de l'information confidentielle

- a) L'utilisateur ne doit pas recourir aux outils de collaboration à des fins d'échanges d'informations confidentielles² concernant un usager s'il existe des processus d'affaires prévus à cet effet. En cas d'absence de tels processus d'affaires, le MSSS autorise l'utilisation des outils de collaboration à cette fin;
- b) L'utilisateur doit informer ses collaborateurs de la nature des informations échangées sur la plateforme des outils de collaboration, notamment leur degré de sensibilité et de criticité;
- c) L'utilisateur peut partager ses informations avec des personnes légitimes, externes à la plateforme des outils de collaboration. Dans ce cas, il devra ajouter aux informations partagées une couche de sécurité supplémentaire (Chiffrement, anonymisation, restreindre les accès, etc.). L'utilisateur doit suivre les bonnes pratiques de partage vers l'externe en vigueur;
- d) L'utilisateur doit s'assurer de la légitimité de ses interlocuteurs en portant une attention particulière à leur identité;
- e) L'utilisateur doit limiter la durée de la présence des informations confidentielles, sur la plateforme des outils de collaboration;
- f) L'utilisateur reconnaît que les informations échangées sur la plateforme des outils de collaboration demeurent la propriété de l'organisme auquel il est rattaché. L'organisme peut user, le cas échéant, de son droit de regard s'il estime qu'un préjudice a été, ou pourrait être, commis.

3.1.2 Règle non limitative d'utilisation progressive de la vidéo

Le recours à la vidéoconférence lors des échanges doit être restreint et utilisé que lorsque les circonstances s'y prêtent. La capacité Internet du MSSS et du RSSS ne peuvent supporter un très grand nombre de connexions vidéo simultanées.

3.1.3 Règles relatives aux contrôles d'accès aux outils de collaboration

- a) L'utilisateur ne doit pas utiliser les identifiants (utilisateur/mot de passe, jeton téléaccès, etc.) d'une autre personne afin de se livrer à des activités, en violation des lois et règlements en vigueur;

² Une information confidentielle est définie comme étant une information à caractère personnel, médical, social, ou toute autre information que l'organisation considère comme telle.

- b) L'utilisateur ne doit pas désactiver ou contourner volontairement les dispositifs de protection en place;
- c) L'utilisateur doit veiller à la protection de ses justificatifs d'identité permettant d'accéder à la plateforme des outils de collaboration;
- d) L'utilisateur doit immédiatement aviser le centre de service de son établissement, ainsi que son gestionnaire, s'il estime que ses justificatifs d'identité ont été, ou pourraient être, violés ou compromis, et ce, dans le respect des politiques et directives du MSSS et du RSSS en matière de déclaration des incidents.

3.1.4 Règles relatives à la catégorisation³ des informations

L'utilisateur doit prendre connaissance de la catégorisation des informations ou documents partagés sur la plateforme des outils de collaboration, préalablement à tout échange. En l'absence de catégorisation, l'utilisateur doit s'abstenir de partager et en aviser le RSI⁴ de son établissement.

3.1.5 Règles relatives au chiffrement

- a) L'utilisateur doit appliquer des mécanismes de chiffrement sur des documents dont le niveau de sensibilité ou de criticité est élevé;
- b) L'utilisateur doit recourir aux mécanismes de chiffrement offerts par son organisation.

3.1.6 Règles relatives à la gestion documentaire et à la conservation des documents

- a) Les informations, échangées sur la plateforme des outils de collaboration, relatives au dossier d'un usager doivent être versées dans son dossier de santé;
- b) L'utilisateur ne peut utiliser la capacité de stockage des outils de collaboration à des fins d'archivage ou de gestion documentaire;
- c) L'utilisateur doit retirer de la plateforme des outils de collaboration les informations n'ayant plus d'utilité, le cas échéant, la stratégie d'expiration s'appliquerait.

³ Exercice consistant à attribuer un degré de sensibilité et de criticité à une donnée, dans le but d'en déterminer le niveau de protection eu égard aux risques encourus en matière de disponibilité, d'intégrité et de confidentialité (DIC)

⁴ Responsable de la sécurité de l'information.

3.1.7 Règles relatives à l'utilisation des appareils mobiles⁵

- a) Les outils de collaboration offrent des facilités d'accès multiplateformes (téléphones intelligents, tablettes, etc.), l'utilisateur doit, par conséquent, prendre les précautions nécessaires afin de garantir la sécurité des informations qu'il détient lorsqu'il transige sur ce type de plateforme (codes Pin⁶, schémas de verrouillage, chiffrement, verrouillage automatique de l'écran, réseau WIFI, Bluetooth, etc.);
- b) L'utilisateur doit s'assurer d'une nette séparation entre ses informations personnelles et professionnelles;
- c) L'utilisateur doit cesser immédiatement d'utiliser les appareils mobiles, s'il suspecte la présence d'un code malicieux ou d'une anomalie. Il doit, en outre, informer le centre de service de l'établissement auquel il est rattaché, en respect des procédures en place⁷.

3.1.8 Pratiques recommandées

L'utilisateur doit se conformer aux pratiques recommandées d'utilisation des outils de collaboration, émanant du Ministère ou de l'établissement auquel il est rattaché.

3.1.9 Sensibilisation des utilisateurs à la sécurité des services infonuagiques

L'utilisateur doit consulter et suivre les recommandations d'utilisation des outils de collaboration, véhiculées par les capsules de formation⁸, offertes par le MSSS.

3.1.10 Déclaration d'incident de sécurité de l'information

L'utilisateur doit immédiatement signaler au centre de service de son établissement tout acte susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie survenue sur la plateforme des outils de collaboration dont il a connaissance.

⁵ Les règles relatives à l'utilisation des appareils mobiles viennent s'ajouter à celles déjà définies par les organismes et établissements du RSSS

⁶ Le code pin ne doit pas être trivial

⁷ MSSS-DIR01 Déclaration des incidents de sécurité - 2015-08-17

⁸ <https://msss365.sharepoint.com/sites/MSSS-Collaboration-SPO/SitePages/Formation.aspx>

3.2 Termes et conditions spécifiques

Les règles découlant des termes et conditions spécifiques à chaque outil de collaboration viennent compléter celles découlant des termes et conditions générales.

3.2.1 Termes et conditions – Outlook

Le MSSS offre à ses utilisateurs et ceux du RSSS, un service de messagerie électronique (Outlook) à usage professionnel, qui permet d'établir une communication interne ou externe, reposant sur des règles de sécurité. Microsoft Outlook offre également des fonctionnalités permettant la gestion de l'agenda, des contacts, des tâches, etc.

L'utilisateur d'Outlook doit particulièrement veiller au respect des règles de sécurité suivantes :

- a) Tout utilisateur doit faire preuve de vigilance en évitant d'ouvrir un courriel de provenance inconnue ou douteuse;
- b) L'utilisateur doit privilégier l'utilisation de son courriel professionnel pour les communications relatives à son travail;
- c) L'utilisation de la messagerie électronique à des fins personnelles ne peut, sans autorisation du ROSI⁹ ou du RSI, permettre l'usage pour des activités commerciales, de publicité ou de sollicitation;
- d) Le MSSS ou l'établissement se réserve le droit d'effectuer un contrôle a posteriori de l'utilisation de la messagerie qui ne pourra porter que sur des indications générales de fréquence, de volume, de taille des messages, du format des pièces jointes, ou sur le contenu des messages échangés;
- e) L'utilisateur ne doit pas utiliser la messagerie électronique à des fins de harcèlement ou pour véhiculer des messages à caractère raciste, pornographique, pédophile, injurieux, diffamatoire ou autres et, de manière générale, à ne pas diffuser d'informations présentant une infraction aux lois et règlements en vigueur;
- f) L'utilisateur ne doit pas extraire, reproduire, ni diffuser les informations à caractère personnel présentes sur l'annuaire du MSSS ou de son établissement à des tiers;
- g) L'utilisateur ne doit pas volontairement effectuer des opérations pouvant porter préjudice au fonctionnement d'Outlook (envoi de document volumineux, envoi massif, etc.).

⁹ Responsable organisationnel de la sécurité de l'information. Uniquement le MSSS détient ce rôle.

3.2.2 Termes et conditions – Microsoft TEAMS

Microsoft Teams est un espace de travail basé sur des échanges instantanés de conversations, de fichiers, de notes ou de tâches permettant de faciliter la collaboration et la communication entre les utilisateurs. Teams intègre certaines fonctionnalités d'Outlook, de SharePoint Online, de OneNote, entre autres.

Règles à adopter lors des conversations

- a) L'utilisateur doit faire preuve de courtoisie, de sobriété et de concision lors de ses échanges;
- b) L'utilisateur ne doit pas abuser de l'utilisation des émoticônes et autres modules GIF, leur utilisation doit rejoindre l'esprit professionnel qui régit la fonction publique québécoise;
- c) L'utilisateur ne doit pas inviter d'autres personnes à une conversation, sans en informer préalablement tous les participants;
- d) L'utilisateur, créateur et propriétaire d'une équipe sur Teams, agit à titre de modérateur de l'équipe, il doit veiller aux règles de sécurité et d'éthique lors des échanges et mettre à jour la liste des participants. Il doit en outre procéder périodiquement à la révision des membres de son équipe, nommer un propriétaire de substitution et respecter les règles de nomenclature établie par le MSSS¹⁰;
- e) Une fois les travaux finis, le propriétaire de l'équipe doit retirer l'équipe et sauvegarder la documentation.

Règles à adopter lors des échanges de documents

- f) L'utilisateur ne doit pas déposer de fichiers trop volumineux sur la plateforme, l'espace alloué étant limité;
- g) L'utilisateur doit appliquer les mesures de sécurité liées aux droits d'accès sur les fichiers partagés¹¹;
- h) Bien que Teams offre une grande capacité de stockage de fichiers, l'utilisateur doit périodiquement procéder au nettoyage de son espace de travail.

Réunions

- i) Comme énoncé à l'article 3.1.2 Règle non limitative d'utilisation progressive de la vidéo, l'utilisateur ne doit pas recourir automatiquement à la visioconférence, il doit en faire un usage modéré.

¹⁰ Voir Norme d'appellation des groupes

¹¹ <https://msss365.sharepoint.com/sites/MSSS-Collaboration-SPO/SitePages/Formation.aspx>

4. Droit de regard

Le ministère de la Santé et des Services sociaux exerce, en conformité avec la législation et la réglementation en vigueur, un droit de regard sur tout usage des actifs informationnels du Réseau.

5. Sanctions

Lorsqu'un utilisateur contrevient ou déroge aux dispositions du présent document, il s'expose selon le cas, à des mesures disciplinaires, administratives ou légales en fonction de la gravité de son geste.

6. Dispositions finales

Les présents termes et conditions entrent en vigueur le