POLITIQUE

PO-18-005	**Utilisation des Services de Messagerie Électronique (SMÉ) à l'égard des informations nominatives à caractère personnel.**	
Direction responsable : DRTI	**Entrée en vigueur : 2020-05-12**	
☒ **Politique organisationnelle** ☐ **Politique spécifique**		**Révisée le :**
Destinataires : Tous les membres du personnel, les médecins et stagiaires du CIUSSS du Nord-de-l'Île-de-Montréal		
Document(s) associé(s) : Utilisation_courrier_electronique_PO-18-005.docx		

1. PRÉAMBULE

Le ministère de la Santé et des Services sociaux (MSSS) offre un service de messagerie électronique (SMÉ) à l'intention de ses employés du réseau de la santé et des services sociaux (RSSS) qui désirent échanger des informations entre eux ou avec les fournisseurs externes. Ce SMÉ à usage strictement professionnel repose sur un ensemble de règles énoncées dans le présent document. Le SMÉ est l'un des moyens de communication utilisés dans le RSSS, pour faciliter l'échange d'information.

2. BUT

Cette politique informe sur le cadre à l'intérieur duquel se retrouve le courrier électronique dans le RSSS. Elle vise à assurer que :

- Les usagers du RSSS sont informés des limites d'application des différentes politiques et lois sur le courrier électronique
- Le SMÉ est utilisé en accord avec ces politiques et lois
- La sécurité, l'intégrité, la disponibilité et l'authenticité des informations sont respectées
- Les usagers du SMÉ sont informés sur la manière dont les concepts de sécurité, de confidentialité, de disponibilité et de respect de la vie privée s'appliquent au courriel
- Le SMÉ est utilisé de manière adéquate et conforme à l'éthique
- L'information nécessaire au bon fonctionnement et à la constitution de la mémoire de l'organisme est préservée et accessible
- L'efficacité et l'efficience des communications internes et externes soient améliorées

3. OBJECTIFS

Cette politique consiste à établir des mesures de sécurité priorisées par le MSSS pour s'assurer de la sécurité logique des actifs informationnels.

La politique vise à encadrer l'utilisation du SMÉ. Elle énonce à cet égard des règles d'utilisation, au regard de la sécurité de l'information, de la protection des renseignements personnels et du code d'éthique en vigueur.

4. DÉFINITIONS

Données confidentielles

Qualifie toute information sensible couvrant des sphères d'activité non connues du grand public, propriété ou non du CIUSSS du Nord-de-l'Île-de-Montréal (CIUSSS NIM). La diffusion de cette information se limite aux personnes ou entités autorisées puisque sa divulgation pourrait offrir un avantage concurrentiel à une tierce partie ou compromettre les opérations ou la sécurité interne de notre établissement.

Données confidentielles nominatives

Ensemble des données propres à un individu qui, une fois combinées, permettent de l'identifier directement ou indirectement.

5. CONTEXTE LÉGAL ET/OU CONTRACTUEL

Cette politique s'appuie sur :

- La politique de Sécurité de l'Information du CIUSSS NIM (PO-18-001)
- La loi concernant le cadre juridique des technologies de l'information (Chapitre C-1.1)
- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, c. M-19.2, a. 5.2);
- La Loi sur le Ministère de la Santé et des Services sociaux (RLRQ, c. M-19.2, a. 5.2);
- La Loi concernant le partage de certains renseignements de santé (RLRQ, c. P-90001, a. 4 et 5);
- La Loi sur la santé et les services sociaux (RLRQ, c. S-4.2) détermine le rôle d'un établissement de santé et traite également de la sécurité des actifs informationnels (AI).
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels

6. CHAMP D'APPLICATION

Cette politique s'applique à tout le personnel du CIUSSS NIM, les employés, les gestionnaires, les médecins, les résidents en médecine, les chercheurs, les étudiants, les bénévoles, les mandataires, les fournisseurs ainsi qu'à ceux qui interviennent pour leur compte et qui utilisent le service de messagerie électronique en place.

7. MODALITÉS

7.1 Les outils

Le ministère de la Santé et des Services sociaux (MSSS) met à la disposition de tous les usagers de la messagerie électronique la suite *Microsoft Office 365* et son logiciel *Outlook*[1].

Tous les logiciels de cette suite sont disponibles sous forme de *SaaS (Software as a Service)* et utilisent le concept d'infonuagique[2] (cloud).

7.2 Les données, courriels et documents-joints

Les données, courriels et documents qui sont annexés aux courriels, sont stockés dans l'infonuagique chez le fournisseur de service Microsoft. L'accès en est contrôlé par une authentification appropriée.

7.3 Disponibilité du service

Le service de messagerie électronique est disponible en tout temps en autant qu'un accès à l'Internet soit possible à partir du poste de travail ou de l'équipement mobile. La disponibilité du service en tout temps est assurée par Microsoft.

7.4 Persistance des données

Les courriels envoyés sont sauvegardés et peuvent demeurer accessibles pendant une période indéterminée. Ce n'est pas parce qu'on le supprime dans notre boîte de courriels que le message est définitivement supprimé du serveur; il peut demeurer disponible aussi longtemps que nécessaire aux destinataires à qui on l'a envoyé.

7.5 La protection des renseignements personnels

En vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, tous les courriels échangés entre membres du personnel sont la propriété du CIUSSS. De plus, ces mêmes courriels sont assujettis à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q. c.A2.1).

C'est pourquoi :

- Bien que Microsoft certifie que les données de la suite Office 365 sont chiffrées de bout en bout (en transit et au repos), les usagers de la messagerie électronique doivent prendre conscience qu'aucun système ne garantit le risque zéro.

  Il est donc recommandé quand cela est possible de favoriser l'utilisation de systèmes d'information clinico-administratifs appropriés, quand il est nécessaire

[1] Outlook est le logiciel client de courrier électronique propriétaire édité par Microsoft.
[2] L'infonuagique correspond à l'accès à des services informatiques via internet.

d'échanger et sauvegarder des informations nominatives ou à caractère personnel.

L'utilisateur doit également porter une attention particulière aux destinataires, ceci afin d'en préserver la confidentialité.

- Le SMÉ offre des facilités d'accessibilité 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 utilise ce type d'équipement.

- Tout utilisateur doit faire preuve de vigilance en évitant d'ouvrir un courriel de provenance inconnue ou douteuse.

- Le MSSS ou l'établissement se réserve le droit d'effectuer un contrôle *a posteriori* de l'utilisation de la messagerie qui pourra porter sur des indications générales de fréquence, de volume, de taille des messages, du format des pièces jointes ou sur le contenu des messages échangés.

- L'utilisateur ne doit pas volontairement effectuer des opérations pouvant porter préjudice au fonctionnement du SMÉ. Citons comme exemples, sans s'y limiter :
  - L'envoi massif de courriels;
  - L'envoi des documents trop volumineux pour prévenir le risque de saturation des boîtes de réception et des serveurs;
  - L'envoi de documents suspects (infectés d'un virus).

- Bien qu'ils transitent sur un canal sécurisé (TLS), les courriels envoyés à l'extérieur du RSSS ne sont pas chiffrés, par défaut. Une fois arrivés à destination, ces messages seront reçus en texte clair. En particulier, si vous transmettez des informations à caractère personnel ou confidentiel, il est essentiel de forcer manuellement le chiffrement de contenu de message, qui est une option disponible dans *Microsoft Outlook*.

- À retenir : Les courriels sont des véhicules de propagation de logiciels malveillants.

8. RÔLES ET RESPONSABILITÉS

Utilisateur (demandeur)

- Faire la demande d'accès au réseau à son cadre supérieur immédiat.
- Appliquer les mesures énoncées dans la présente politique.

Cadre supérieur immédiat

- Valider la demande des droits d'accès au réseau de ses employés.

- Informer le service informatique et les ressources humaines du départ prolongé ou définitif d'un employé.
- Appliquer les mesures énoncées dans la présente politique.

9. RÉVISION

La révision de ce document doit être effectuée tous les 3 (trois) ans, à partir de la date d'adoption ou avant, lors de changements majeurs dans l'organisation de la sécurité. Un exercice de consultation doit être effectué et le même processus d'adoption s'applique, qu'il y ait des modifications ou non.

10. PRÉCISIONS

ÉLABORATION :	Jean-François Fortin Conseiller Cadre en Sécurité de l'Information - RSI DRTI
COLLABORATION :	
ANNULE ET REMPLACE :	Hôpital du Sacré-Cœur-de-Montréal Politique A.G.-032 Utilisation des services du réseau Internet et du courrier électronique
ADOPTÉ PAR : **DATE** : **NO. RÉSOLUTION**	
RÉVISION (année) :	2023