Centre intégré universitaire de santé et de services sociaux de l'Est-de-l'Île-de-Montréal
Québec

Direction générale adjointe

POLITIQUE

UTILISATION DE L'INFONUAGIQUE PUBLIQUE		
Nº Politique : **POL-059**	Responsable de l'application : Responsable de la sécurité de l'information (RSI)	
Nº Procédure découlant : **s.o.**		
Approuvée par : **Comité de direction**	Date d'approbation : **2018-03-27**	Date de révision : **2022-03-27**
Destinataires : Toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire ou de fournisseur, utilise les actifs informationnels du CIUSSS-EMTL ou y a accès.		

1. CONTEXTE

La présente politique a pour objet d'établir les conditions dans lesquelles les utilisateurs autorisés des actifs informationnels du CIUSSS de l'Est-de-l'Île-de-Montréal (EMTL) peuvent utiliser les plateformes infonuagiques, telles que Smartsheet, Microsoft Office 365, Dropbox, Microsoft OneDrive, Google Drive ou la messagerie électronique publique, dans le cadre de leurs fonctions.

Les préoccupations du point de vue de la sécurité dans le nuage comprennent celles qui suivent :

- vol de données ou piratage;
- question de droit (si les données sont stockées dans un autre pays, il se peut qu'une législation différente sur l'accès à l'information autorise le gouvernement à y accéder);
- fiabilité du fournisseur (compétence, responsabilité, mesures de sécurité) et solvabilité;
- accès aux données réservées au personnel autorisé;
- pressentiment que la sécurité des renseignements personnels est susceptible d'être compromise (basé par exemple sur l'historique du fournisseur en matière de sécurité, sur les risques des utilisations prévues de la plateforme, sur les attaques avérées ou potentielles).

Les affaires électroniques sont régies par la Loi sur la protection des renseignements personnels et les documents électroniques[1] ainsi que par certaines dispositions

[1] L.C. 2000, ch5

prévues dans d'autres lois, normes et exigences (Annexe 1). Des recours en justice peuvent être intentés contre le CIUSSS-EMTL si, pour quelque motif que ce soit, la sécurité des renseignements personnels de nos usagers, employés et partenaires est compromise.

Les utilisateurs doivent donc s'assurer de protéger toute information en prenant soin de se conformer à la présente politique, découlant de la politique de sécurité de l'information du CIUSSS-EMTL (POL-024).

2. CHAMP D'APPLICATION

La présente politique s'applique aux utilisateurs des actifs informationnels, c'est-à-dire à toute personne œuvrant au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut d'employé que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

L'information visée est celle que le CIUSSS-EMTL détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers, incluant entre autres les informations sur les usagers ou les employés, les documents administratifs ou professionnels.

3. OBJECTIFS

L'objectif de la présente politique est de protéger les informations détenues par le CIUSSS-EMTL, lors de l'utilisation de services publics en infonuagique, des risques d'accès non autorisés, de la perte, du vol ou de la divulgation à l'insu du CIUSSS-EMTL.

La politique permet d'identifier :

- ce qui peut être utilisé et stocké dans les services publics infonuagiques;
- les contrôles de sécurité qui doivent être mis en place afin de protéger les actifs informationnels du CIUSSS-EMTL;
- les personnes autorisées qui peuvent consulter et modifier les informations du CIUSSS-EMTL.

4. DÉFINITIONS

4.1. Espace de stockage

Terme générique employé pour désigner une infrastructure utilisée pour le stockage de documents numériques. Le réseau informatique du CIUSSS-EMTL, les services hébergés au Centre de services régional, la plateforme infonuagique privée de l'organisme ou une plateforme infonuagique publique (sur Internet) constituent des espaces de stockage.

4.2. Infonuagique

Modèle de prestation de services de technologie de l'information qui permet aux utilisateurs d'accéder à des ressources résidant sur Internet par l'entremise d'outils

et d'applications Web, plutôt qu'au moyen d'une connexion directe à un serveur du CIUSSS-EMTL ou du Réseau intégré de télécommunication multimédia (RITM).

Cette prestation de services permet un accès, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services évolutifs, adaptables dynamiquement et facturés ou non à l'utilisation; par exemple : Microsoft Office 365, Dropbox ou Google drive.

- **Infonuagique publique**

  Infrastructure de stockage publique exploitée par un tiers, soit en dehors du RITM et du réseau du CIUSSS-EMTL, et disponible en mode libre-service à des fins personnelles ou commerciales. L'utilisateur peut y accéder par Internet, ou encore par une application installée sur son équipement; les données sont stockées sur Internet.

  L'infonuagique publique peut être gratuite ou payante selon le fournisseur ou selon la capacité d'utilisation désirée. Par exemple : Microsoft Office 365, Dropbox, Google Drive, iCloud, OneDrive, Smartsheet.

4.3. Renseignements confidentiels (ou information confidentielle)

Sont confidentiels les renseignements personnels au sens de la loi[2], relatifs aux usagers et aux personnels du CIUSSS-EMTL, le tout conformément aux lois et règlements en vigueur.

Sont également considérés comme confidentiels au sens de la loi : tout renseignement dont la divulgation aurait des incidences sur les négociations entre organismes publics[3], un secret industriel[4], un renseignement industriel, financier, commercial, scientifique ou technique[5], l'administration de la justice et la sécurité publique[6], les décisions administratives ou politiques[7] et la vérification[8].

4.4. Renseignement personnel[9]

Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la Politique de sécurité de l'information (POL-024) du CIUSSS-EMTL.

---

[2] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1, art 53
[3] Ibid., art 20.
[4] Ibid., art 22 (1).
[5] Ibid., art 22 (2) et 23.
[6] Ibid., art 28 et ss.
[7] Ibid., art 30 et ss.
[8] Ibid., art 41 et ss.
[9] Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1 [Loi sur l'accès]

Note[10] : Les renseignements personnels suivants ont un caractère public : le nom, le titre, la fonction (incluant le numéro d'employé[11]), la classification (du poste), l'échelle de traitement (échelle salariale, mais non le salaire), les coordonnées du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction.

4.5. Répertoire personnel

Emplacement réseau alloué à une personne et dont les droits d'accès sont restreints à cette seule personne. Souvent identifié par une lettre (exemple « F: »).

4.6. Répertoire commun

Emplacement réseau alloué à un groupe de personne ayant les mêmes tâches ou devant accéder aux mêmes informations dans le cadre de leurs fonctions, et dont les droits d'accès sont restreints à ce même groupe (exemple « B: »).

4.7. Réseau intégré de télécommunications multimédia (RITM)

L'infrastructure de communication du réseau de la santé, soit le RITM, permet l'échange sécuritaire et confidentiel de données entre les différents établissements et professionnels, et permet également l'accès et le filtrage contrôlés à l'Internet.
La Direction générale des technologies de l'information du ministère de la Santé et des Services sociaux (DGTI-MSSS) assure la gestion opérationnelle du réseau de télécommunications en plus des divers services s'y reliant, notamment : téléaccès (télétravail), visioconférence, accès pour les fournisseurs externes (service F).

4.8. Utilisateur

Toute personne œuvrant au sein du CIUSSS-EMTL, de quelque catégorie d'emploi et de statut d'employé que ce soit, les médecins, les médecins résidents, les dentistes, les pharmaciens, les chercheurs, le personnel de soins et services, administratif ou de soutien, les pairs aidants, les stagiaires, les bénévoles, ainsi que toute personne physique ou morale qui, par engagement contractuel ou autrement, utilise un actif informationnel du CIUSSS-EMTL ou y a accès.

5. ÉNONCÉ

5.1. Règles fondamentales d'utilisation des plateformes d'infonuagique publique

Les plateformes d'infonuagique publique peuvent être utilisées, au besoin, pour le stockage et la transmission d'information NON confidentielle.

Ces outils ne doivent pas servir à stocker ou transmettre d'information confidentielle (par exemple : information nominative, personnelle, non publique et toute information sur les usagers), à moins qu'aucun moyen sécurisé autorisé par le CIUSSS-EMTL, soit par la Direction des ressources technologiques (DRT) et le responsable de la sécurité de l'information (RSI), ne soit disponible et que la situation ne l'exige autrement.

[10] Ibid., art 57 (1)
[11] Selon la jurisprudence émanant de la Commission d'accès à l'information

Les règles suivantes s'appliquent en tout temps pour l'utilisation de ces moyens; la prudence est toujours requise lors de l'utilisation de ces outils de partage de l'information non sécurisés.

L'information sur les employés (sauf celle déclarée publique, voir la rubrique 4.5) et toute l'information sur les usagers – même leur nom – est hautement confidentielle et ne doit donc pas être inscrite dans ces outils non sécurisés de partage de données.

Afin d'éviter de divulguer de l'information confidentielle sur ces plateformes non sécurisées, si elles sont utilisées alors qu'aucun autre moyen sécurisé et autorisé n'est disponible et que la situation l'exige, il est plus approprié d'utiliser le numéro de dossier d'employé ou le numéro de dossier d'usager, sans aucune autre donnée permettant d'identifier ces personnes.

5.2. Règles pour le choix de l'espace de stockage et le moyen de transmission de l'information

À moins qu'aucun moyen sécurisé autorisé par le CIUSSS-EMTL (soit par la DRT et le RSI) ne soit disponible et que la situation ne l'exige autrement :

- aucun utilisateur du CIUSSS-EMTL ne doit stocker ou transmettre d'information confidentielle sur une plateforme infonuagique publique (par esemple : Smartsheet, Dropbox, Google drive); se référer à la définition d'un renseignement confidentiel ou information confidentielle de la rubrique 4.5;

- toute information confidentielle doit être stockée en tout temps sur le réseau informatique protégé du CIUSSS-EMTL (répertoire personnel de l'utilisateur, répertoire commun, ou sur les services hébergés du CIUSSS-EMTL);

- toute information confidentielle doit être transmise en tout temps par les outils fournis et autorisés par le CIUSSS-EMTL (par exemple : le lecteur de partage réseau du CIUSSS-EMTL, le courriel du CIUSSS-EMTL, en suivant les procédures de sécurité requises);

- l'utilisateur ne doit pas utiliser de boîte de courriel publique (par exemple : Gmail, Hotmail) pour échanger des informations confidentielles, ni d'ailleurs pour tout besoin dans le cadre de ses fonctions;

- l'utilisateur doit se conformer en tout temps aux bonnes pratiques et utiliser les moyens mis à sa disposition par le CIUSSS-EMTL pour transmettre toute information confidentielle de façon sécuritaire à l'extérieur du (RITM);

- l'utilisateur doit utiliser la procédure de transmission des informations confidentielles du CIUSSS-EMTL.

5.3. Procédure de demande d'accès aux services de l'infonuagique publique autorisés

L'utilisateur doit se référer à la procédure d'accès aux plateformes infonuagiques publiques autorisées par le CIUSSS-EMTL (par exemple : Smartsheet, Dropbox, Microsoft OneDrive, Google Drive), soit en résumé :

- Une demande d'autorisation pour l'utilisation d'un outil infonuagique public doit être acheminée au Centre de services informatiques de la DRT par le gestionnaire en charge de l'utilisateur, selon la procédure régulière de demande d'accès.

- La DRT se chargera d'évaluer le besoin de l'utilisateur et d'offrir une orientation si nécessaire.

- S'il n'a pas été signé et acheminé au préalable, le formulaire[12] d'engagement à la confidentialité et au respect de l'éthique à l'égard des actifs informationnels dûment signé par l'utilisateur, doit être joint à la demande, en format numérique.

- Sur approbation par la DRT de l'accès demandé, l'utilisateur pourra dès lors utiliser son compte d'infonuagique publique.

5.4. Sauvegarde des données sur toute plateforme infonuagique publique

Le CIUSSS-EMTL ne peut avoir accès à l'information déposée sur les plateformes infonuagiques publiques et ne possède donc aucun mécanisme de recouvrement des données qui y sont entreposées.

Aussi, les utilisateurs du CIUSSS-EMTL qui se servent de ces plateformes doivent s'assurer d'avoir des copies de sauvegarde, en cas de corruption ou de perte accidentelle d'un document entreposé sur une plateforme d'infonuagique publique.

5.5. Protection des accès à l'espace de stockage sur toute plateforme d'infonuagique publique

L'utilisateur de la plateforme d'infonuagique publique ne doit jamais partager ses codes d'accès et mots de passe avec un autre utilisateur ou un tiers externe, conformément à la politique de gestion des accès (POL-058). L'utilisateur de l'infonuagique a la possibilité de faire des partages de répertoire ou de fichier avec ses collaborateurs, mais les collaborateurs doivent utiliser leur propre compte dans l'application, afin d'accéder aux informations partagées.

L'utilisateur a l'obligation de contrôler le niveau d'accès qu'il attribue aux autres utilisateurs du CIUSSS-EMTL et de l'externe, et de révoquer rapidement les droits des autres utilisateurs qui ne doivent plus accéder aux informations. Selon les possibilités de la plateforme, il sera également possible de journaliser les accès aux informations partagées pour audits.

5.6. Sanctions

Lorsqu'un utilisateur contrevient ou déroge à la présente politique, il s'expose notamment à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement, la fin de contrat, la fin de stage ou autre, et ce, conformément aux dispositions des conventions collectives, des ententes ou des contrats.

[12] Annexé à la Politique de sécurité de l'information POL-024.

Le CIUSSS-EMTL peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou règlement en vigueur a été commise.

6. RÔLES ET RESPONSABILITÉS

6.1. La direction générale adjointe – Finances, soutien, administration et performance (DGA-FSAP)

Le comité de la sécurité de l'information recommande le contenu de la présente politique de sécurité de l'information au comité de direction pour approbation via la DGA-FSAP.

6.2. Le comité de direction

Il adopte les politiques de sécurité de l'information établies par le CIUSSS-EMTL et ses mises à jour, et en suit l'application.

6.3. Le responsable de la sécurité de l'information (RSI)

Il veille à la communication, à la compréhension et l'application par les principaux intervenants, les autres responsables désignés et les utilisateurs, des politiques de sécurité de l'information du CIUSSS-EMTL.

6.4. Les directions des ressources humaines, des communications et des affaires juridiques (DRHCAJ), de l'enseignement universitaire, de la recherche et de la logistique

Elles sont responsables, notamment, d'informer toute nouvelle personne œuvrant au sein du CIUSSS-EMTL ou tout nouveau fournisseur ou partenaire du CIUSSS-EMTL, sous leur responsabilité, dès son accueil ou le début de son mandat, de ses obligations découlant des politiques en vigueur en matière de sécurité de l'information.

6.5. La Direction des ressources technologique (DRT)

La DRT est responsable d'émettre les procédures complémentaires à la présente politique, pour le volet technologique, et de veiller à la gestion et à la prise en charge des activités qui la concernent, découlant de cette politique.

6.6. Toutes les directions

Elles sont responsables de la mise en œuvre, auprès de toute personne œuvrant au sein du CIUSSS-EMTL et relevant de leur autorité, des dispositions des politiques de sécurité de l'information du CIUSSS-EMTL (POL-024).

6.7. Les utilisateurs

Tel que stipulé à la politique de sécurité de l'information du CIUSSS-EMTL, les utilisateurs ont l'obligation de se conformer aux politiques, procédures et règlements du CIUSSS-EMTL.

Ils ont également l'obligation de signaler immédiatement selon la procédure de déclaration d'incident de sécurité de l'information, tout acte ou situation dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des

règles de sécurité, ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CIUSSS-EMTL.

7. ÉLABORATION, RÉDACTION ET MISE À JOUR DE LA POLITIQUE

7.1. Le responsable de la sécurité de l'information (RSI)

Le RSI est responsable de s'assurer de l'élaboration, de la rédaction et de la mise à jour de la politique, en collaboration avec la DRT.

7.2. Comité de sécurité de l'information

Les membres du comité de sécurité de l'information ont participé à la validation de la politique, et participent à la validation de sa mise à jour.

7.3. Calendrier de révision de la politique

La présente politique devra être révisée tous les 4 ans ou plus rapidement en fonction des besoins.

8. RESPONSABLE DE LA MISE EN APPLICATION

8.1. Le responsable de la sécurité de l'information (RSI)

Il est responsable de la mise en application de la présente politique.

9. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur le jour de son adoption par le comité de direction et annule, par le fait même, toute autre politique en cette matière adoptée antérieurement dans l'une ou l'autre des installations administrées par le CIUSSS-EMTL.

10. ANNEXE(S)

ANNEXE 1 – Cadre légal et administratif de la sécurité de l'information.

ANNEXE 1 - Cadre légal et administratif de la sécurité de l'information

La présente politique s'inscrit principalement dans un contexte régi par les lois, codes et règlements suivants :

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ c G-1.03

Loi concernant le cadre juridique des technologies de l'information, RLRQ c C-1.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ c A-2.1

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ c P-39.1

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5

Loi sur les services de santé et les services sociaux, RLRQ c S-4.2

Loi modifiant l'organisation et la gouvernance du réseau de la santé et des services sociaux notamment par l'abolition des agences régionales, RLRQ c O-7.2

Code des professions, RLRQ c C-26

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ c A-2.1, r 2

Charte des droits et libertés de la personne, RLRQ c C-12

Code civil du Québec, RLRQ c CCQ-1991

Loi sur les archives, RLRQ c A-21.1

Loi canadienne sur les droits de la personne, LRC 1985, c H-6

Code criminel, LRC 1985, c C-46.