BONNES PRATIQUES RELATIVES AU TÉLÉTRAVAIL DANS LE CONTEXTE EXCEPTIONNEL COVID-19

Version	1.0
Date de création	16/03/2020
Date d'application	17/03/2020
Durée d'application	Jusqu'à la fin des mesures règlementant les déplacements dans le cadre de la lutte contre la propagation du virus Covid-19
Champ d'application	Les bonnes pratiques sont diffusées à l'ensemble du personnel du GHICL amené à télétravailler, que ce soit depuis un poste professionnel ou personnel.

En raison du passage au stade 3 de l'épidémie de COVID-19, certains personnels sont conduits à accéder aux serveurs depuis leur domicile, à partir d'un poste professionnel ou d'un poste personnel (ci-après, « les utilisateurs »).

Nous vous rappelons que cet accès à distance, depuis un poste personnel, présente un caractère exceptionnel, et qu'il est interdit en dehors du contexte de pandémie.

Ce contexte de connexion et d'utilisation fait peser un risque concernant le fonctionnement, la sécurité et l'intégrité du système d'information du GHICL, mais également concernant les données (à caractère personnel ou non, sensibles ou non) traitées dans le cadre de l'activité du service.

Compte tenu du caractère sensible des données traitées, chaque utilisateur se doit de :

- ✓ Faire preuve de la plus grande **vigilance** possible concernant leur protection ;
- ✓ **Veiller à ce que des tiers non autorisés n'aient pas connaissance de telles données**, conformément aux règles d'éthique professionnelle, de déontologie, et de protection des données personnelles.

***L'utilisateur s'engage à respecter les recommandations ci-dessous émises dans ce contexte exceptionnel*.**

Mesures de sécurité générales

- ⇨ **Ne pas se connecter sur des réseaux sans-fils libres** type « hotspot » (lieux publics, gares, *etc*.), réseaux non fiables de par leur nature
- ⇨ S'assurer du bon fonctionnement et du bon état de santé du matériel personnel utilisé (antivirus, mise à jour, etc.)
- ⇨ **Verrouiller son poste** lors de toute interruption du travail (pause, déjeuner, fin de journée), le raccourci suivant peut être utilisé : appuyer simultanément sur les touches Windows et L
- ⇨ **Débrancher** les **assistants vocaux**
- ⇨ Ne pas copier de documents professionnels, notamment de documents contenant des données médicales depuis le serveur sur le poste personnel
- ⇨ **Ne pas connecter de support amovible** (chargeur de téléphone, clé USB, disque dur, etc.) sur l'ordinateur lorsque la session Citrix est ouverte
- ⇨ **Ne pas communiquer par téléphone des situations relevant du secret médical**

L'utilisateur est tenu d'informer sans délai l'administrateur de tout dysfonctionnement, altération, perte, vol, destruction et autre évènement pouvant affecter les moyens informatiques et de communication électronique

Mots de passe

- ⇨ Ne divulguer le mot de passe à aucune autre personne
- ⇨ Ne pas conserver le mot de passe sous une forme aisément accessible à des tiers (Ex : post-it)

Réception et envoi de messages électroniques

- ⇨ S'assurer de l'identité de l'émetteur ou du destinataire du message avant d'ouvrir toute pièce-jointe ou de cliquer sur un lien
- ⇨ Ne pas communiquer des données médicales via la messagerie personnelle, les réseaux sociaux ou au moyens de plateformes de stockage en ligne, ces supports n'étant pas sécurisés

Vigilance

! Des campagnes de **phishing** ont été détectées au travers d'e-mails malveillants avec pour thématique le coronavirus (ex : « consultez en temps réel les cas de coronavirus », questionnaires de santé, etc.)

Nous vous demandons de prêter une attention toute particulière à l'usage des réseaux sociaux, des **mails personnels** et des environnements **Drive** personnels depuis les ordinateurs du GHCIL.

Administrateur

De manière générale, l'administrateur a pour mission d'assurer le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication. Il a ainsi accès aux logs de connexion et aux adresses IP de tout équipement (professionnel ou personnel) se connectant aux serveurs du service.