UNIVERSITÉ DE GENÈVE
DIRECTION DU SYSTÈME D'INFORMATION

Directive relative aux services numériques dans le cadre du télétravail, dite « Directive Numérique & Télétravail »

Remarque préliminaire : cette version de la directive est une version préliminaire de travail mise à disposition dans le cadre du pilote télétravail 2019. Des modifications ultérieures pourront être amenées pour tenir compte des enseignements tirés de cette phase pilote.

Cette directive synthétise les recommandations qui concernent l'écosystème numérique mis à disposition des télétravailleurs-euses.

Ressources numériques et télétravail

L'Université de Genève met à disposition de chaque télétravailleur-euse un ensemble de services et de ressources numériques nécessaires et suffisants dans le cadre du télétravail :

- Un accès distant sécurisé au réseau interne de l'Université ;
- Un ordinateur mobile (si déjà fourni dans le cadre de la relation de travail) ou un poste de travail virtuel préconfiguré (sinon) ;
- Un service de téléphonie VoIP ;
- Une documentation complète ;
- Un service d'accompagnement et de support.

Modalités de connexion distante

Pour se connecter de manière distante au réseau de l'Université – et ainsi accéder à l'ensemble des services numériques internes –, les télétravailleurs-euses doivent utiliser le service d'authentification forte de l'Université ISIs+ qui permet de se protéger efficacement des accès de tiers non autorisés aux données sensibles de l'Université.

Dans ce cadre, 2 modes de connexion sont possibles :

- Utilisation d'un équipement informatique institutionnel, et d'une connexion VPN.
- Utilisation d'un équipement informatique privé et d'une connexion VDI sécurisée.

Les postes de travail virtuels sont préconfigurés selon les besoins généraux évitant ainsi l'installation et la configuration des applications standard.

Il est à noter que l'utilisation directe du VPN sur un équipement privé est interdite car elle ne permet pas de garantir une utilisation maîtrisée en termes de support informatique, de gestion des licences, de protection des données notamment personnelles, de qualité de service globale et d'expérience utilisateur.

Il est à noter également qu'il reste possible dans le cadre de l'itinérance, c'est-à-dire dans le cadre d'un accès distant ponctuel, d'accéder sans authentification forte aux services web standard tels que le portail institutionnel, la messagerie électronique, ou les plateformes d'enseignement.

Exigences relatives aux équipements

Équipement informatique institutionnel

Le poste de travail institutionnel mobile utilisé par le/la télétravailleur-euse doit être « *managé* », c'est-à-dire qu'il doit être préalablement :

- enregistré dans l'annuaire d'entreprise,
- configuré avec les outils standards de gestion et de configuration du poste,
- sécurisé par l'activation des mesures de protection standard (antivirus, pare-feu, chiffrement du poste, etc.).

Chaque télétravailleur-euse peut se rapprocher de son correspondant informatique pour s'en assurer, et ce avant de débuter son télétravail.

En cas de perte ou de vol du poste de travail institutionnel mobile, le/la télétravailleur-euse doit informer le service STEPS.

Équipement informatique privé

Dans le cas de l'utilisation d'un équipement informatique privé, les exigences du chapitre 4 « Utilisation responsable d'équipements de type Bring your Own Device (BYOD) » de la charte d'usage des ressources numériques s'appliquent. On considère ici, non seulement les ordinateurs fixes ou mobiles, mais également les tablettes et smartphones.

En particulier, chaque télétravailleur-euse s'engage à :

- utiliser un système informatique récent et à jour ;
- utiliser un logiciel anti-malware à jour ;
- s'assurer du bon fonctionnement de son équipement ;
- ne pas enregistrer de données de travail sur son équipement BYOD mais seulement dans les espaces de stockage de données de l'Université prévus à cet effet, via le poste de travail virtuel ;
- signaler au support informatique de l'Université tout problème de sécurité rencontré lors d'une session de télétravail.

Seule l'installation des logiciels de téléphonie (Jabber) et de connexion distante sécurisé (VDI Horizon) est autorisée sur les équipements BYOD.

Dans ce cadre, l'Université propose un service de support spécifique pour le télétravail encadré selon la Politique de support informatique des équipements privés (BYOD).

Téléphonie et visioconférence

L'Université met à disposition un service gratuit de téléphonie VoIP (softphone). Ceci permet l'utilisation du numéro de téléphone institutionnel du/de la télétravailleur-euse qu'il/elle soit en session de télétravail

ou non. L'utilisation du téléphone privé du/de la télétravailleur-euse et la transmission du numéro de téléphone privé ne sont donc pas nécessaires.

Le logiciel de téléphonie peut être installé sur les équipements institutionnels ou privés et ne nécessite pas l'utilisation de l'authentification forte. L'acquisition d'un casque pour softphone ou d'une webcam est à la charge de l'entité de rattachement de chaque télétravailleur-euse.

Un usage strictement professionnel de ce service de téléphonie est attendu.

Dispositions complémentaires

Chaque télétravailleur-euse s'engage à respecter dispositions suivantes :

- Ne pas donner accès à des tiers ou des proches aux outils et données de travail, et notamment ne pas laisser sa session de travail ouverte sans contrôle ;
- Ne pas imprimer de contenus sensibles ou confidentiels au domicile mais seulement à l'UNIGE.
  La sensibilité des informations est déterminée par chaque métier sur son domaine de responsabilité selon la classification de l'information définie dans la politique de sécurité du système d'information ;
- Ne pas enregistrer de données de travail via des messageries privées ou des services Cloud grand public de stockage et de gestion de données mais seulement via les services institutionnels ;
- Ne pas transmettre ses données personnelles (numéro de téléphone personnel, adresse mail privée, …). Le cadre de télétravail permet de l'éviter.

D'une manière générale, les conditions et exigences de l'article 25 « Utilisation du téléphone et des ressources informatiques » du Règlement sur le personnel de l'Université, et de la charte d'usage des ressources numériques s'appliquent également dans le cadre du télétravail.

Des recommandations de bonnes pratiques complètent ces dispositions.