

ANNEXE 3 : SECURISATION DES DONNEES DANS LE CADRE DU TELETRAVAIL EN EPLE

Des mesures doivent être mises en œuvre pour assurer la protection des données personnelles de l'agent en télétravail et de celles traitées par celui-ci à des fins professionnelles, dans le respect du règlement général pour la protection des données (RGPD) et des prescriptions de la CNIL.

A ce titre, le poste de travail doit vérifier les conditions minimales de fonctionnement suivantes :

1. **Mise à jour régulière du système et des logiciels**
Le système d'exploitation et tous les logiciels installés doivent être régulièrement mis à jour afin de corriger les failles de sécurité potentielles.
2. **Antivirus et anti-malware**
Le poste doit disposer d'un programme antivirus fiable et constamment maintenu à jour pour détecter et neutraliser les menaces.
3. **Utilisation de mots de passe forts**
L'agent doit respecter la politique en matière d'accès aux services numériques du ministère de l'éducation, à savoir des mots de passe à 12 caractères et 4 classes. L'utilisation d'un gestionnaire de mots de passe peut aider à générer et stocker les mots de passe de manière sécurisée.
4. **Chiffrement des données**
Le disque dur de l'ordinateur doit être chiffré, la clé de déchiffrement déposée sous coffre pour protéger les données en cas de perte ou de vol de l'appareil.
5. **Sécurité du réseau**
Le poste de travail doit utiliser un réseau privé virtuel (VPN) pour sécuriser la connexion via l'Internet pour accéder au système d'information de l'établissement (*).
6. **Sensibilisation et formation à la sécurité numérique**
 - Le chef d'établissement doit s'assurer que tous les utilisateurs sont informés des pratiques de sécurité élémentaire, telles que ne pas ouvrir des pièces jointes ou des liens d'emails suspects et éviter les sites web non sécurisés (*).
 - L'agent est invité à effectuer des sauvegardes régulières des données importantes sur des supports externes ou des services cloud sécurisés (apps.education.fr) et le serveur administratif de l'établissement pour éviter la perte de données en cas d'incident.
 - Politiques de sécurité strictes :
 - i. Le poste ne doit pas être en mode administrateur lors des sessions quotidiennes.
 - ii. Le poste de travail ne doit être utilisé que par l'agent qui en assume la responsabilité.
 - iii. Tous les moyens d'accès au système d'information de l'établissement doivent être qualifiés par l'équipe RSSI de l'académie

(*) Le SMIB peut intervenir dans le processus de qualification et de sécurisation du poste devant servir au télétravail après conventionnement. (à partir de aout/septembre 2024)

Procédure de mise en place du télétravail

Liaison EPLE - DSI

