Sécuriser son poste de travail

Pour minimiser les risques liés à l'utilisation de votre ordinateur et les failles de sécurité, il est conseillé de (selon les directives 6.1 et 6.6) :

- **Contacter le Help desk en cas de doute**
- Protéger son ordinateur avec un mot de passe administrateur unique
- Tenir à jour son ordinateur:
  - Appliquer les mises à jour logiciel
  - Appliquer les mises à jour système (≠ passer à un nouveau système d'exploitation, ce qui est conseillé après que l'éditeur ait publié une version x.2 ou 2 mises à jour mineures de son nouvel OS => défauts de jeunesse et compatibilité avec l'essentiel des principaux logiciels du marché en principe assurée, la vérification de la compatibilité avec des logiciels métiers relève néanmoins de la responsabilité de l'utilisateur)
  - Travailler sur un OS maintenu par l'éditeur et donc au bénéfice de régulières mises à jour de sécurité
- Utiliser les logiciels de sécurité de votre système d'exploitation:
  - Sous macOS, le logiciel XProtect est intégré et activé par défaut, pour le personnel sous contrat UNIL le Ci propose en supplément la solution Microsoft Defender for EndPoint (protection accrue de la machine et du réseau UNIL)
  - Sous Windows, Windows Defender est activé par défaut si vous n'utilisez pas un autre logiciel antivirus, le Ci propose également Microsoft Defender for EndPoint pour le personnel sous contrat UNIL (protection accrue de la machine et du réseau UNIL)
- Sauvegarder régulièrement vos données sur un support externe (le service Sauvegarde poste de travail propose gratuitement au personnel UNIL sous contrat un logiciel de sauvegarde automatique des données sur des serveurs UNIL)
- Suivre les règles de sécurité suivantes:
  - Ne jamais télécharger des fichiers de sites web dont on ne connait pas la provenance
  - Ne jamais installer des logiciels de développeurs inconnus
  - Ne jamais ouvrir les pièces jointes d'expéditeurs inconnus (particulièrement les fichiers se terminant par: .exe, .js)
  - Ne jamais répondre aux emails demandant de renvoyer des données confidentielles
- Utiliser des mots de passe uniques pour tous ses comptes (privés et professionnels):
  - Il existe des gestionnaires de mots de passe qui facilitent ce travail
- Mesures particulières à prendre si vous utilisez un laptop que vous déplacez régulièrement ou si vous faites du télétravail (directive 1.40):
  - si vous stockez des données personnelles ou sensibles au sens de la directive 6.9 vous avez l'obligation de chiffrer les données de votre disque, afin d'interdire à un tiers d'accéder à ces informations (par exemple en cas de vol ou de perte de la

machine)
    - sur Mac utilisez FileVault (intégré à macOS)
    - sur Windows utilisez BitLocker (intégré à Windows)
    - attention à sauvegarder en lieu sûr la clé de chiffrement générée sous peine de ne plus pouvoir accéder à vos données
- si vous vous trouvez en dehors du réseau UNIL vous avez l'obligation de chiffrer vos communications pour empêcher un tiers malintentionné de les intercepter, en utilisant le VPN crypto mis à disposition par l'UNIL.
- pour se prémunir des vols ne jamais laisser son laptop sans surveillance.

Révision #3
Créé 24 mars 2026 10:06:11 par Karim Khouw Zegwaart
Mis à jour 28 avril 2026 06:29:37 par Karim Khouw Zegwaart