

BONNES PRATIQUES: TRAVAIL À DISTANCE

1 Sécuriser sa connexion internet

- **Utiliser un VPN** : Chiffre vos données et protège votre navigation
- **Éviter les Wi-Fi publics (cafés, hôtels)** : Privilégiez une connexion filaire
- **Sécuriser son réseau domestique** :
 - Modifier le mot de passe Wi-Fi par défaut
 - Activer le chiffrement WPA3 ou WPA2.
 - Mettre à jour le routeur régulièrement

3 Se prémunir contre le phishing et l'ingénierie sociale

- **Vérifier l'expéditeur des e-mails** : Se méfier des demandes urgentes et inhabituelles.
- **Ne jamais cliquer sur un lien suspect** :
 - **Vérificateur de liens suspects** :
 - **VirusTotal** - Scanne les URLs et pièces jointes
 - **URLVoid** - Vérifie la réputation des liens (détecte les sites web malicieux)
 - **Hybrid Analysis** - Analyse comportementale des fichiers
 - **Vérificateur d'expéditeur** :
 - **Have I Been Pwned** - Vérifie si l'adresse a été compromise
 - **Whois Lookup** - Informations sur les domaines suspects
- **Ne pas partager d'informations sensibles** : Par e-mail, téléphone ou messagerie instantanée.
- **Signaler tout e-mail suspect** : À l'équipe TI ou au responsable TI

2 Sécuriser ses appareils et ses outils de travail

- **Verrouiller son ordinateur** : Activer un mot de passe robuste ou l'authentification biométrique
- **Mettre à jour ses logiciels** : Système d'exploitation, antivirus, applications
- **Utiliser un antivirus et un pare-feu** : Protège contre les malwares et intrusions
- **Éviter les périphériques USB inconnus** : Risque de malware (clé USB piégée).
- **Utiliser uniquement les outils approuvés par l'entreprise** : Messagerie, stockage cloud, visioconférence.
- **Activer l'authentification multi-facteurs (MFA)** : Sécuriser les accès aux applications sensibles.
- **Ne pas enregistrer ses mots de passe dans le navigateur** : Privilégier un gestionnaire de mots de passe sécurisé.
- **Verrouiller son écran lors d'une absence même courte (windows + L)** :
 - Protège l'accès non autorisé à votre ordinateur et à vos données lorsque vous n'êtes pas devant.
 - Empêche des modifications accidentelles ou intentionnelles par une personne qui passerait devant votre poste.
 - Maintenir la confidentialité de ce qui est affiché sur votre écran.
- **Stockage sécurisé** :
 - Utilisez les solutions de stockage officielles (OneDrive, SharePoint, etc.)
 - Évitez de stocker des documents sensibles sur des supports non sécurisés (clés USB personnelles).
- **Évitez d'installer des applications personnelles sur votre poste professionnel**
- **Ne pas partager son écran sans vérifier les informations affichées** : Risque de fuite de données
- **Éviter les conversations sensibles dans des lieux publics** : Espionnage possible via micro ou caméra

BONNES PRATIQUES: PARTAGE DE DOCUMENTS À L'EXTERNE

1 Avant de partager un document: Les questions à se poser

Questions

Exemples

- | | |
|--|---|
| • Ce document est-il confidentiel? | Données RH, données clients |
| • Le partage est-il vraiment nécessaire ? | Si possible, ne donner qu'un extrait ou un résumé. |
| • Suis-je autorisé à partager ce contenu ? | Respecter les règles internes de classification informationnelle. |

2 Partage par pièce jointe (email)

- **Limiter la taille des fichiers** : <10 Mo pour éviter les problèmes de livraison.
- **Formater les fichiers correctement** :
 - Ex: PDF ou DOCX,
 - éviter les formats exotiques (.exe, .bat).
- **Chiffrer les pièces sensibles** : Utiliser un ZIP avec mot de passe (envoyé séparément)
- **Nommer les fichiers clairement** :
 - Ex: Contrat_Client_XYZ_2025.pdf au lieu de doc_final3_versiondef.pdf

3 Partage via OneDrive / Google Drive / autres plateformes cloud

Gestion des Accès et Permission

- **Principe du moindre privilège** :
 - Accordez uniquement les droits nécessaires (lecture, modification, commentaire)
 - Préférez "Lecture seule" par défaut pour les consultations
 - Utilisez "Modification" uniquement pour la collaboration active
 - Évitez les droits "Propriétaire" sauf cas exceptionnels
- **Contrôle des destinataires** :
 - Partagez avec des adresses email spécifiques, jamais "Toute personne avec le lien"
 - Vérifiez l'adresse email avant l'envoi
 - Utilisez les groupes de sécurité plutôt que les partages individuels multiple

Limitation temporelle

- **Expiration automatique** :
 - Définissez toujours une date d'expiration (10, 30, 60, 90 jours maximum)
 - Renouvelez explicitement si nécessaire
 - Programmez des rappels pour réviser les accès
- **Révocation proactive** :
 - Retirez l'accès dès la fin du projet
 - Auditez régulièrement les partages actifs
 - Supprimez les accès des collaborateurs qui quittent l'entreprise.

Classification et Organisation

- **Nommage standardisé** :
[CONFIDENTIALITE][PROJET][VERSION][DATE]
Ex: **CONFIDENTIEL_Budget2024_v2.1_20251201**
- **Structure de dossiers** :
 - Créez une hiérarchie claire et logique
 - Séparez les documents par niveau de confidentialité
 - Utilisez des noms de dossiers explicites

⚠ Erreurs Courantes à Éviter

- **À ne jamais faire** :
 - Partager avec "Toute personne avec le lien"
 - Utiliser des plateformes personnelles (Dropbox perso, Onedrive perso etc.)
 - Oublier de définir une date d'expiration
 - Envoyer des documents sensibles sans protection
 - Ignorer les notifications d'accès suspects

Sécurité Renforcée

- **Protection par mot de passe** :
 - Activez systématiquement pour les documents sensibles
 - Communiquez le mot de passe par un canal séparé (SMS, appel)
 - Utilisez des mots de passe complexes et uniques (voire aide-mémoire sur les mots de passe)
- **Paramètres de sécurité** :
 - Désactivez le téléchargement pour les documents très sensibles
 - Interdisez le partage en cascade (re-partage par les destinataires)
 - Activez les notifications d'accès et de modification

✅ Réflexes à adopter :

- ✓ Toujours vérifier avant de cliquer "Partager"
- ✓ Tester l'accès avec un compte test
- ✓ Documenter les raisons du partage
- ✓ Former régulièrement les équipes

📋 Check-list Avant Partage

- ☐ **Le document est-il classifié correctement ?**
- ☐ **Le destinataire a-t-il vraiment besoin d'accès ?**
- ☐ **Les droits sont-ils au minimum nécessaire ?**
- ☐ **Une date d'expiration est-elle définie ?**
- ☐ **Un mot de passe est-il requis ?**
- ☐ **Le partage est-il tracé et approuvé ?**
- ☐ **Les notifications sont-elles activées ?**