

TIP 2.9

Sauvegarder, restaurer et transférer les données d'un utilisateur

Fiche de révision - Équipements numériques

1. Les 4 notions à distinguer

Action	Principe
Copie	Dupliquer des fichiers vers un autre emplacement.
Sauvegarde	Créer une copie permettant une restauration après perte ou incident.
Synchronisation	Maintenir des données cohérentes entre plusieurs emplacements.
Transfert	Déplacer ou recopier les données vers un nouvel environnement.

Méthode à retenir :

Identifier → Sauvegarder → Contrôler → Restaurer → Tester → Faire valider → Documenter

2. Identifier les données

Ne pas supposer que tout se trouve dans Documents. Examiner le profil utilisateur, les dossiers non standards, les données applicatives spécifiques, les espaces réseau et les emplacements synchronisés.

Emplacement / donnée	Point de vigilance
Bureau / Documents / Images	Données courantes du profil utilisateur.
Téléchargements	À trier : peut contenir des fichiers temporaires ou inutiles.
AppData	Ne pas recopier intégralement sans procédure applicative.
Partage réseau	Vérifier si la donnée est déjà centralisée.
Espace synchronisé	Contrôler l'état réel de synchronisation et la restaurabilité.

3. Destination et confidentialité

Règle essentielle : utiliser uniquement un stockage autorisé par l'organisation. Éviter clé USB personnelle, cloud personnel ou PC privé. Accéder uniquement aux données nécessaires à l'intervention.

4. Robocopy

Commande / option	Utilité
robocopy "Source" "Destination" /E	Copie l'arborescence, y compris les dossiers vides.
/R:2	Limite les nouvelles tentatives en cas d'échec.
/W:2	Attend 2 secondes entre les tentatives.
/LOG:fichier.log	Conserve une trace du résultat de la copie.
/MIR	Miroir : peut supprimer sur la destination ce qui n'existe plus à la source. À utiliser avec prudence.

5. Contrôler la sauvegarde

Une copie terminée n'est pas forcément une sauvegarde validée. Vérifier la présence des dossiers, les erreurs du journal, le volume copié et l'ouverture de plusieurs fichiers représentatifs.

Contrôle	Exemple
Nombre de fichiers	(Get-ChildItem ... -File -Recurse).Count
Empreinte d'un fichier	Get-FileHash fichier -Algorithm SHA256
Ouverture	Tester plusieurs documents importants sur la destination.

6. Restaurer réellement

Une sauvegarde n'a de valeur que si les données peuvent être restaurées. Tester la restauration d'un fichier dans un emplacement temporaire, l'ouvrir, vérifier son contenu puis documenter le résultat.

7. Principe 3-2-1 et redondance

Notion	À retenir
3-2-1	Principe courant : 3 copies, 2 types/emplacements de stockage, 1 copie séparée du système principal.
RAID	Améliore la disponibilité selon sa configuration, mais ne remplace pas une sauvegarde.
Synchronisation	Peut répliquer une suppression ; ne remplace pas automatiquement une sauvegarde historisée.

8. Migration vers un nouveau poste

Étape	Action
1	Identifier les données locales, réseau et synchronisées.
2	Sauvegarder les données locales nécessaires.
3	Préparer le nouveau poste.
4	Restaurer ou laisser resynchroniser selon la procédure.
5	Tester les fichiers et données applicatives.
6	Faire valider par l'utilisateur avant effacement de l'ancien poste.

9. Chiffrement et disque défaillant

Avant toute opération, vérifier si le stockage est chiffré et si les mécanismes de récupération prévus sont disponibles. Sur un disque présentant des signes sérieux de panne, limiter les écritures inutiles : la priorité devient la protection des données.

Commande utile : Get-BitLockerVolume permet de consulter certaines informations BitLocker sur les volumes.

10. Checklist avant effacement de l'ancien poste

Contrôle	État attendu
Données locales	Recensées et sauvegardées.
Synchronisation	Terminée et sans erreur connue.
Données applicatives	Traitées selon la procédure de l'application.
Restauration	Données disponibles sur le nouveau poste.
Tests	Fichiers importants ouverts avec succès.
Utilisateur	A validé que ses données essentielles sont présentes.
Ancien poste	Effacement uniquement selon la procédure après validation.

11. À retenir

La sauvegarde doit être contrôlée et restaurable.
Identifier précisément les données, protéger leur confidentialité, utiliser une destination autorisée, contrôler la copie, tester la restauration et ne jamais effacer l'ancien poste avant validation.