|  |
| --- |
|  |
| Documentation d’Exploitation |
| CHU de Ynov |

|  |
| --- |
| VIOLLET Yoan, ETESSE Tristan |

# 1. Accès et gestion des sauvegardes

Les sauvegardes des données critiques (dossiers médicaux, bases de données, configurations systèmes) sont effectuées automatiquement selon le planning suivant :  
- Sauvegarde quotidienne des bases actives (incrémentielle)  
- Sauvegarde complète hebdomadaire (chaque dimanche à 3h00)  
  
Les sauvegardes sont chiffrées et stockées sur un serveur de stockage sécurisé hors site.  
  
Accès aux sauvegardes :  
- Emplacement : serveur de stockage [\backup\chu-ynov]  
- Authentification requise via compte administrateur  
- Logiciel utilisé : rsync (Linux) ou Veeam (Windows)  
- Journalisation des accès activée  
  
Restaurer une sauvegarde :  
- Accéder au dossier concerné selon la date de sauvegarde  
- Déchiffrer via la clé fournie au RSSI  
- Copier les fichiers vers le serveur cible  
- Redémarrer les services associés

# 2. Déclenchement du Plan de Reprise d’Activité (PRA)

En cas de sinistre ou d’indisponibilité majeure (attaque, panne), le PRA doit être déclenché par le RSSI ou l’administrateur système de garde.  
  
Étapes du PRA :  
1. Diagnostic rapide : identifier les systèmes impactés  
2. Isoler les systèmes compromis (déconnexion réseau)  
3. Préparer l’environnement de secours (VM de secours ou serveur miroir)  
4. Restaurer la dernière sauvegarde valide  
5. Relancer les services essentiels (DNS, AD, bases médicales)  
6. Vérification post-restauration avec le personnel médical  
  
Délai visé : retour des services critiques en moins de 2 heures.

# 3. Réflexes et consignes de sécurité pour le personnel

- En cas de doute sur un mail ou un lien, ne pas cliquer. Signaler immédiatement au service informatique.  
- Ne jamais utiliser de clés USB personnelles.  
- Verrouiller systématiquement sa session dès qu’on quitte son poste.  
- En cas de comportement suspect (ralentissement, fenêtres inconnues), appeler le support.  
- Ne jamais partager ses identifiants, même avec un collègue ou un supérieur.  
- Appliquer les mises à jour dès qu’elles sont proposées par le service informatique.

# 4. Documents utiles et référentiels

- PSSI officielle : disponible sur l’intranet dans la section “Documents sécurité”  
- Fiches réflexes : imprimées dans les services et accessibles en PDF  
- Plan de sensibilisation : consultable par tous les encadrants pour mise en œuvre  
- Planning des sauvegardes : accessible via le tableau de bord IT  
- Contact support sécurité : it-securite@chu-ynov.fr / poste 1234