Documentation Utilisateurs et Administrateurs – Open Pharma

1. Introduction

Cette documentation décrit les nouvelles procédures à appliquer suite à la sécurisation du SI d'Open Pharma. Elle s'adresse :

- aux **utilisateurs** (employés non techniques),
- aux **administrateurs** (équipe IT et sécurité).

Objectif : garantir la **confidentialité, l'intégrité et la disponibilité** des données R&D sensibles, conformément aux recommandations de l'ANSSI.

---

2. Bonnes pratiques générales

Utilisateurs

Chaque utilisateur doit **utiliser uniquement ses propres identifiants**, **se connecter systématiquement via le VPN IPsec avec MFA**, **ne jamais partager son mot de passe**, **installer uniquement les logiciels validés par l'IT** et **signaler immédiatement toute activité suspecte** pour sécuriser le système et éviter les cyberattaques.

Précisions :

- **Description** : Utiliser uniquement les identifiants personnels fournis.
- **Raison** : Empêcher l'usurpation et renforcer la traçabilité.
- **Recommandation ANSSI** : R33.
- **Modification** : Mot de passe personnel, jamais partagé.
- **Description** : Ne pas installer de logiciels sans validation IT.
- **Raison** : Réduire les risques de logiciels malveillants.

- **Recommandation ANSSI** : R13.
- **Modification** : Tous les logiciels doivent être validés par l'équipe IT.
- **Description** : Signaler toute activité suspecte.
- **Raison** : Permet une réaction rapide face aux attaques.
- **Recommandation ANSSI** : R1 (charte SSI).
- **Modification** : Signalement immédiat au support IT.

Administrateurs

- **Description** : Séparer comptes admin / utilisateurs.
- **Raison** : Limiter l'exposition des comptes à privilèges.
- **Recommandation ANSSI** : R27.
- **Modification** : Utilisation obligatoire de comptes distincts.
- **Description** : Appliquer le principe du moindre privilège.
- **Raison** : Réduire l'impact en cas de compromission.
- **Recommandation ANSSI** : R39.
- **Modification** : Limiter les droits au strict nécessaire.
- **Description** : Mettre à jour régulièrement les systèmes.
- **Raison** : Corriger les vulnérabilités.
- **Recommandation ANSSI** : R42.
- **Modification** : Déploiement via relais de mises à jour.

---

3. Modifications réseau et impacts

1. Segmentation en VLAN

- **Description** : Réseau plat remplacé par VLAN par service.
- **Raison** : Cloisonner les flux et réduire les déplacements latéraux.
- **Recommandations ANSSI** : R5, R16.
- **Modification** :
    - Utilisateurs : n'ont accès qu'aux ressources de leur service.
    - Administrateurs : mise à jour ACL et supervision inter-VLAN.

2. Pare-feu NGFW

- **Description** : Ajout d'un pare-feu FortiGate 60F.
- **Raison** : Filtrage avancé.
- **Recommandations ANSSI** : R6, R16, R24.
- **Modification** :
    - Utilisateurs : navigation Internet filtrée.
    - Administrateurs : règles à maintenir et logs supervisés.

3. Mise en place d'une DMZ + Reverse Proxy

- **Description** : Isolation des serveurs exposés avec un reverse proxy Lenovo SR250.
- **Raison** : Protéger les serveurs internes et filtrer les flux web.
- **Recommandations ANSSI** : R18, R19.
- **Modification** :
    - Utilisateurs : accès inchangé via applications métiers.
    - Administrateurs : gestion stricte des flux DMZ ↔ interne.

4. VPN IPsec dédié

- **Description** : Accès distant via tunnel IPsec + MFA.

- **Raison** : Sécuriser les connexions distantes.
- **Recommandations ANSSI** : R15-, R49, R51.
- **Modification** :
    - Utilisateurs : connexion plus longue (mot de passe + token).
    - Administrateurs : VPN termine dans VLAN Admin uniquement.

5. IPS réseau

- **Description** : Déploiement d'un équipement HPE IPS dédié.
- **Raison** : Détecter et bloquer les intrusions réseau en complément du NGFW.
- **Recommandations ANSSI** : R6, R16.
- **Modification** :
    - Administrateurs : surveiller les alertes IPS et corriger les flux suspects.

6. Relais de mises à jour

- **Description** : Serveur WSUS/apt-mirror en DMZ.
- **Raison** : Bloquer accès direct Internet depuis serveurs internes.
- **Recommandations ANSSI** : R43, R44.
- **Modification** :
    - Administrateurs : valider MAJ en préproduction avant déploiement.

7. Sauvegardes sécurisées

- **Description** : NAS dédié + copie hors ligne.
- **Raison** : Protéger contre ransomwares et sinistres.
- **Recommandations ANSSI** : R45.
- **Modification** :

- Administrateurs : vérifier quotidiennement l'intégrité des sauvegardes.

8. Nouvelle version d'Active Directory + Mise à jour Linux (debian)

- **Description** : Mise à jour et durcissement du serveur AD + mise à jour Linux.
- **Raison** : Renforcer l'authentification, compatibilité avec MFA et GPO avancées.(politique de mot de passe fort, complexe avec chiffre, lettre, caractère spécial + changement obligatoire tous les X mois)
- **Recommandations ANSSI** : R27, R30, R36.
- **Modification** :
  - Utilisateurs : authentification renforcée.
  - Administrateurs : gestion centralisée des comptes et politiques renforcée.

9. Flux sécurisés

- **Description** : Chiffrement TLS systématique entre services (SMB, LDAPS, HTTPS).
- **Raison** : Empêcher l'interception des données.
- **Recommandations ANSSI** : R21, R24.
- **Modification** :
  - Utilisateurs : utilisent les applications métiers en HTTPS.
  - Administrateurs : veillent à configurer TLS et certificats à jour.

10. Serveur RADIUS

- **Description** : Mise en place d'un serveur RADIUS pour authentification 802.1X.
- **Raison** : Sécuriser les connexions réseau filaires et Wi-Fi.
- **Recommandations ANSSI** : R15, R36.
- **Modification** :
  - Utilisateurs : connexion automatique via identifiants AD.

- Administrateurs : configuration des switches/points d'accès avec RADIUS.

11. SIEM + outils de collecte de métriques (Supervision)

- **Description** : Déploiement d'une solution intégrée pour :

  Centraliser les logs (SIEM) afin de détecter les anomalies et incidents de sécurité.

  Collecter et visualiser les métriques (supervision) pour surveiller la santé des systèmes, faciliter le debugging et anticiper les pannes.

- **Raison** : Détection rapide des incidents de sécurité (via le SIEM).

  Surveillance proactive des performances et de la disponibilité (via les métriques).

- **Recommandations ANSSI** : R46, R47.
- **Modification** :
  - Utilisateurs : aucun impact direct.
  - Administrateurs : consultation quotidienne et réaction aux alertes.

12. Postes d'administration chiffrés

- **Description** : Séparation stricte des postes bureautiques et postes admin, disques chiffrés.
- **Raison** : Protéger les environnements d'administration.
- **Recommandations ANSSI** : R9, R10, R14.
- **Modification** :
  - Administrateurs : utiliser uniquement les postes dédiés chiffrés, pas d'accès Internet.

13. Chiffrements des disques des PC + Serveurs

- **Raison** : Protéger les données au repos contre le vol ou la compromission physique.
  - **Recommandations ANSSI** : R14.
  - **Modification** :
    - Utilisateurs : aucun impact direct, données protégées.
    - Administrateurs : gestion des clés de chiffrement et déploiement.

14. Antivirus / EDR

- **Description** : Déploiement d’une solution antivirus centralisée avec capacités EDR (Endpoint Detection and Response) sur tous les postes de travail et serveurs.
- **Raison** : Détection et neutralisation des menaces (malwares, ransomwares, attaques zero-day) au niveau des terminaux.
- **Recommandations ANSSI** : R61.
- **Modification** :
    - Utilisateurs : analyse en temps réel des fichiers et applications.
    - Administrateurs : supervision des alertes, gestion des quarantaines et mises à jour des définitions.

15. Plan de Reprise d'Activité (PRA) / Plan de Continuité d'Activité (PCA)

- **Description** : Élaboration et mise en œuvre de procédures de PRA et PCA pour garantir la disponibilité des services critiques en cas d'incident majeur (panne, sinistre, cyberattaque).
- **Raison** : Assurer la résilience du SI et minimiser l'impact d'une interruption d'activité sur les opérations d'Open Pharma, répondant aux exigences organisationnelles et réglementaires.
- **Recommandations ANSSI** : Non spécifiquement une recommandation technique directe, mais s'intègre dans une démarche de gestion des risques globale préconisée.
- **Modification** :
    - Utilisateurs : procédures de travail adaptées en cas de déclenchement du PRA/PCA.
    - Administrateurs : participation aux exercices de PRA/PCA, maintenance des infrastructures de secours et mise à jour des procédures.

---

4. Procédures quotidiennes

Utilisateurs

- Connexion locale : session AD (identifiant/mot de passe).
- Connexion distante : VPN + MFA.
- Accès fichiers : partages réseau sécurisés.
- Messagerie : client officiel ou webmail sécurisé.

Administrateurs

- Connexion admin : poste dédié chiffré + compte séparé (SSH/RDP).
- Mises à jour : via relais DMZ (WSUS/apt-mirror).
- Supervision : suivi NGFW, IPS et SIEM.
- Sauvegardes : contrôle quotidien (NAS + hors ligne).
- Gestion réseau : authentification centralisée via RADIUS.

---

5. Conséquences pour les usagers

- **Utilisateurs** : navigation Internet filtrée, connexion VPN plus contraignante, authentification renforcée (MFA, 802.1X), meilleure protection contre phishing/ransomwares.
- **Administrateurs** : procédures plus strictes (postes admin chiffrés, comptes séparés), supervision centralisée (SIEM, IPS), administration renforcée (nouvel AD, RADIUS), conformité ANSSI accrue.

---

6. Conclusion

La sécurisation du SI introduit des contraintes nouvelles, mais indispensables pour protéger les données stratégiques d'Open Pharma. Chaque modification est directement reliée à une recommandation ANSSI, garantissant la conformité et la robustesse du SI.