Documentation Utilisateurs et Administrateurs

Projet de Sécurisation du SI - OpenPharma

Table des matières

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

1. Introduction et Contexte

Dans le cadre de la mise en conformité avec les recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), le département R&D d'OpenPharma procède à une refonte complète de son architecture réseau et de sécurité.

Cette documentation présente les évolutions majeures qui impacteront vos usages quotidiens, ainsi que les nouvelles procédures à suivre pour maintenir un niveau de sécurité optimal tout en préservant votre productivité.

Objectifs de la sécurisation

- Renforcer la protection contre les cybermenaces
- Améliorer le cloisonnement des données sensibles
- Centraliser l'administration et la supervision
- Garantir la traçabilité des actions administratives

2. Vue d'ensemble des évolutions

2.1 Nouvelle architecture réseau (Recommandations ANSSI R15, R16)

Changement principal : Segmentation complète du réseau en zones de confiance fonctionnelles (VLAN) selon le guide ANSSI "Administration sécurisée des SI" (section 3.2, p.11).

Zone	VLAN	Réseau	Utilisateurs concernés
Direction	VLAN 10	10.100.10.0/24	Laurie Garrido, Béatrice Jean-Robert, Yassine Ouari
Laboratoire	VLAN 20	10.100.20.0/24	Équipes Laby, ImageJ, Avogadro
Études	VLAN 30	10.100.30.0/24	Équipes des applications métier
Technique	VLAN 40	10.100.40.0/24	Hicham Laouini, Cynthia Caouren
Administrateurs	VLAN 50	10.100.50.0/24	Postes d'administration dédiés
Serveurs internes	VLAN 70	10.100.70.0/24	Serveurs d'applications
DMZ	VLAN 110	10.100.110.0/24	Services exposés sur Internet

Impact utilisateur : Votre poste sera automatiquement configuré dans la zone appropriée selon votre fonction.

Note : La cartographie complète du SI avec adressage et matrice des flux est disponible en annexe.

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

2.2 Mise en place d'un bastion d'administration (Recommandations ANSSI R18, R19, R20, R21)

Changement : Conformément aux recommandations ANSSI R18 et R19 (p.25-26), tous les accès administratifs passent désormais par un serveur bastion sécurisé (Teleport) avec interface d'administration dédiée et filtrage strict.

Impact administrateur : Obligation d'utiliser le bastion pour toute administration à distance avec authentification multi-facteurs (MFA) selon la recommandation R36 (p.36).

3. Applications du Département - Nouveaux Comptes et Accès

Le tableau ci-dessous présente les applications actuelles avec leurs nouveaux modes d'accès sécurisés :

Application	Type	Description	Collaborateurs	Nouveaux Comptes
OPharma-B	Généraliste	Application d'accès à la badgeuse	Sylvain Bouchard, Hicham Laouini, Cynthia Caouren, Alexandre Levêque, Asma Ben Omar, Roberto Rivieira, Moussa Camara, Marilyn Chen, Laurie Garrido, Béatrice Jean-Robert, Yassine Ouari, Lyvia Kevain	**Compte personnel du salarié** avec authentification centralisée (**LDAPS)**
OPharma-C	Généraliste	Application d'accès aux congés	Tous les collaborateurs	**Compte personnel du salarié** avec authentification centralisée (**LDAPS)**
OPharma-A	Généraliste	Application d'accès à l'annuaire de l'entreprise	Roberto Rivieira, Moussa Camara, Marilyn Chen, Laurie Garrido, Béatrice Jean-Robert, Yassine Ouari, Lyvia Kevain	**Compte personnel du salarié** avec authentification centralisée (**LDAPS)**
Avogadro	Métier	Outil d'édition et de visualisation de molécules chimiques en 3D	Asma Ben Omar, Roberto Rivieira, Alexandre Levêque, Béatrice Jean-Robert	**Compte personnel du salarié** avec authentification centralisée (**LDAPS)**+ accès VLAN Laboratoire
ImageJ	Métier	Outil de traitement et	Sebastien Devilliers, Asma Ben Omar, Roberto Rivieira,	**Compte personnel du salarié** avec

Application	Type	Description	Collaborateurs	Nouveaux Comptes
		d'analyse d'images pour les applications biomédicales	Lyvia Kevain, Béatrice Jean-Robert	authentification centralisée (**LDAPS)** + accès VLAN Laboratoire
Laby	Métier	Outil de gestion et d'optimisation des processus du laboratoire	Roberto Rivieira, Yassin Ouari, Moussa Camara, Marilyn Chen, Cynthia Caouren, Hicham Laouini	**Compte personnel du salarié** avec authentification centralisée (**LDAPS)** + accès VLAN Laboratoire/Études

4. Nouvelles Procédures pour les Utilisateurs

4.1 Connexion aux applications métier (Recommandation ANSSI R24)

Avant : Connexion HTTP non sécurisée avec comptes personnels **Maintenant :** Connexion HTTPS sécurisée avec authentification centralisée

Selon la recommandation ANSSI R24 (p.30), les protocoles utilisant des mécanismes de chiffrement et d'authentification (HTTPS) sont privilégiés et les protocoles non sécurisés sont désactivés.

Procédure :

1. Ouvrez votre navigateur et accédez à l'application via HTTPS uniquement
2. Utilisez vos identifiants de connexion personnels habituels
3. Acceptez le certificat interne si demandé (certificat validé par notre ADCS)

4.2 Accès aux partages de fichiers (Recommandation ANSSI R24)

Changement : Migration de SMB vers SMB3 chiffré (port 445) conformément à la recommandation ANSSI R24 sur l'utilisation de protocoles sécurisés.

Procédure :

1. Les partages réseau utilisent désormais un protocole chiffré automatiquement
2. **Aucune action requise de votre part**, la connexion reste totalement transparente
3. En cas de problème, contactez l'équipe technique

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

4.3 Impression sécurisée (Recommandation ANSSI R24)

Changement : Migration vers IPPS (Internet Printing Protocol Secure) - port 631, conformément à la recommandation ANSSI R24 sur les protocoles sécurisés.

Procédure :

1. Vos imprimantes seront automatiquement reconfigurées
2. Lors de l'impression, une boîte de dialogue s'ouvrira automatiquement vous demandant vos identifiants de connexion personnels
3. Saisissez votre nom d'utilisateur et mot de passe habituels
4. Les documents sensibles sont désormais chiffrés jusqu'à l'imprimante

Impact : Sécurisation renforcée sans ralentissement notable du processus d'impression.

4.4 Téléphonie IP sécurisée (Recommandation ANSSI R24)

Changement : Migration de SIP vers SIP/TLS avec SRTP pour respecter la recommandation ANSSI R24 sur l'utilisation de protocoles sécurisés.

Impact :

- Communications vocales entièrement chiffrées pour une sécurité renforcée
- **Aucun changement dans votre utilisation quotidienne** : décrochez et composez comme d'habitude
- Qualité audio préservée, transparence totale pour l'utilisateur

5. Nouvelles Procédures pour les Administrateurs

5.1 Accès au bastion d'administration (Recommandations ANSSI R18, R19, R27, R30, R36)

Équipement requis : Clé FIDO2 (fournie par l'entreprise) conformément à la recommandation R36 sur l'authentification double facteur.

Procédure de connexion :

1. Connectez-vous depuis un poste du VLAN Administrateurs dédié (10.100.50.0/24) - Recommandation R15
2. Accédez au bastion via HTTPS : https://bastion.openpharma.local
3. Authentifiez-vous avec vos identifiants d'administration dédiés + clé FIDO2 (Recommandations R27, R30)

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

4. Sélectionnez la ressource cible dans l'interface Teleport

Ressources accessibles depuis le bastion :

- Serveurs Linux : SSH (port 22)
- Serveurs Windows : RDP (port 3389)
- Interfaces d'administration : HTTPS (port 443)
- Administration Windows distante : WinRM HTTPS (port 5986)

Important : Conformément aux recommandations R19 et R20, seuls les flux depuis les postes d'administration vers les ressources administrées sont autorisés, aucun rebond entre ressources n'est possible.

5.2 Gestion des mises à jour (Recommandations ANSSI R42, R43, R44)

Nouveau processus centralisé conformément au MCS (Maintien en Condition de Sécurité) :

Pour Windows :

1. Utilisez le serveur WAPT relais (10.100.70.X) déployé en DMZ selon R43
2. Validez les correctifs en environnement de recette avant déploiement (R44)
3. Respectez la fenêtre de maintenance hebdomadaire
4. Documentez toute procédure d'urgence selon R44

Pour Linux :

1. Utilisez apt-cacher-ng (10.100.70.X) comme serveur relais selon R43
2. Testez sur serveur de développement avant production
3. Appliquez la qualification des correctifs selon R44
4. Documentez chaque mise à jour critique

Processus de veille : Mise en place d'une veille technologique systématique selon R42 pour identifier les mises à jour de sécurité critiques.

5.3 Accès VPN sécurisé (Recommandations ANSSI R19, R20, R21, R24)

Nouvelle solution : IPsec/IKEv2 avec authentification par certificat RSA conformément aux recommandations R21 et R24 sur le chiffrement des flux d'administration.

Configuration :

1. Installation du certificat client fourni par l'ADCS interne
2. Configuration du client VPN (profil fourni par l'équipe)

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

3. **Connexion obligatoire vers le bastion uniquement** (pas d'accès direct aux ressources) - Recommandations R19, R20

Ports utilisés : UDP 500/4500 + protocole ESP

Sécurité renforcée : Authentification mutuelle par certificats et chiffrement de bout en bout selon les standards ANSSI.

6. Supervision et Journalisation (Recommandations ANSSI R46, R47)

6.1 Nouveau système de supervision

Infrastructure mise en place conformément aux exigences ANSSI :

- **SIEM Wazuh** : Analyse en temps réel des événements de sécurité
- **Syslog TLS** : Centralisation chiffrée des journaux (port 6514) selon R24
- **NTP interne** : Synchronisation temporelle fiable pour l'horodatage selon R46

6.2 Éléments surveillés

Pour tous les utilisateurs (Recommandation R46) :

- Tentatives de connexion aux applications avec horodatage
- Accès aux partages de fichiers sensibles liés à l'identité
- Utilisation des imprimantes avec traçabilité
- Trafic réseau anormal

Pour les administrateurs (Recommandation R47) :

- **Toutes les sessions SSH/RDP sont enregistrées** avec captures d'écran
- **Commandes administratives tracées** avec contenu détaillé
- Accès aux interfaces d'administration journalisés
- **Collecte centralisée** de toutes les traces d'administration

Important : Ces mesures respectent les recommandations ANSSI R46-R47 sur la journalisation complète, horodatée et intègre des actions d'administration. L'objectif est la protection de l'entreprise et la traçabilité réglementaire.

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

7. Sauvegardes Sécurisées (Recommandation ANSSI R45)

7.1 Nouvelle stratégie 3-2-1 conforme ANSSI

Architecture respectant la recommandation R45 sur la sauvegarde hors ligne :

- **Sauvegarde primaire** : Veeam Backup & Replication sur serveurs
- **Stockage local sécurisé** : NAS Synology avec snapshots immutables
- **Copie externe hors ligne** : Réplication chiffrée vers cloud avec rclone

7.2 Impact utilisateur

- **Partages personnels :** Sauvegarde automatique quotidienne transparente
- **Données métier :** Sauvegarde continue avec rétention de 30 jours
- **Restauration :** Demande via ticket, traitement sous 4h ouvrées
- **Sécurité :** Les éléments critiques disposent d'une sauvegarde hors ligne selon R45

8. Bonnes Pratiques de Sécurité

8.1 Pour tous les utilisateurs

Mots de passe :

- Utilisez exclusivement vos identifiants de connexion personnels
- Ne partagez jamais vos identifiants
- Signalez immédiatement tout problème d'authentification

Navigation :

- Vérifiez la présence du cadenas HTTPS avant de saisir des identifiants
- Acceptez uniquement les certificats de l'entreprise
- Signalez les alertes de sécurité du navigateur

Postes de travail :

- Verrouillez votre session lors des absences
- N'installez pas de logiciels sans autorisation
- Respectez la politique de chiffrement des supports amovibles

8.2 Pour les administrateurs

Comptes d'administration (Recommandations ANSSI R27, R29, R30) :

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

- Utilisez **exclusivement vos comptes d'administration dédiés** distincts de vos comptes utilisateur
- **Usage exclusif pour les actions d'administration** (pas d'usage personnel)
- **Comptes individuels** attribués à chaque administrateur

Clés FIDO2 (Recommandation ANSSI R36) :

- Conservez votre clé principale en lieu sûr
- Utilisez la clé de secours uniquement en cas de perte
- Signalez immédiatement toute perte ou vol

Administration (Recommandations ANSSI R39, R40, R41) :

- Respectez le **principe du moindre privilège**
- Privilégiez l'attribution de **droits aux groupes** plutôt qu'aux comptes
- Ne mélangez jamais usage personnel et professionnel sur les postes admin
- Appliquez les **politiques de sécurité** définies

Bastion (Recommandations ANSSI R18, R19, R20) :

- Fermez systématiquement vos sessions après utilisation
- Ne laissez pas de sessions ouvertes sans surveillance
- Documentez les actions administratives importantes
- Respectez l'interdiction de rebond entre ressources administrées

9. Support et Contacts

9.1 Équipe technique

Support niveau 1 : Cynthia Caouren (Technicienne)

- Email : c.caouren@openpharma.fr

Support niveau 2 : Hicham Laouini (Administrateur systèmes)

- Email : h.laouini@openpharma.fr

Chef de projet sécurité : Maël BENE

- Email : m.bene@openpharma.fr

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr

9.2 Procédure d'incident

En cas de problème :

1. Tentez les solutions de base (redémarrage, reconnexion)
2. Contactez le support niveau 1 via ticket
3. Pour les urgences sécurité : contactez directement Hicham ou Maël

Délais de traitement :

- Incident bloquant : 2h ouvrées
- Demande standard : 24h ouvrées
- Évolution : 5 jours ouvrés

Cette documentation sera mise à jour régulièrement. Version actuelle : 1.0 du 06/09/2025

Pour toute question, contactez l'équipe projet à : securite@openpharma.fr