FICHE DE BONNES PRATIQUES

Protégez les données et l'environnement informatique de votre pharmacie

Les récentes alertes de cybersécurité dans les officines nous rappellent l'importance de protéger les données de santé de vos patients, vos données métier et votre système informatique.

Quelques gestes simples permettent de réduire significativement les risques.

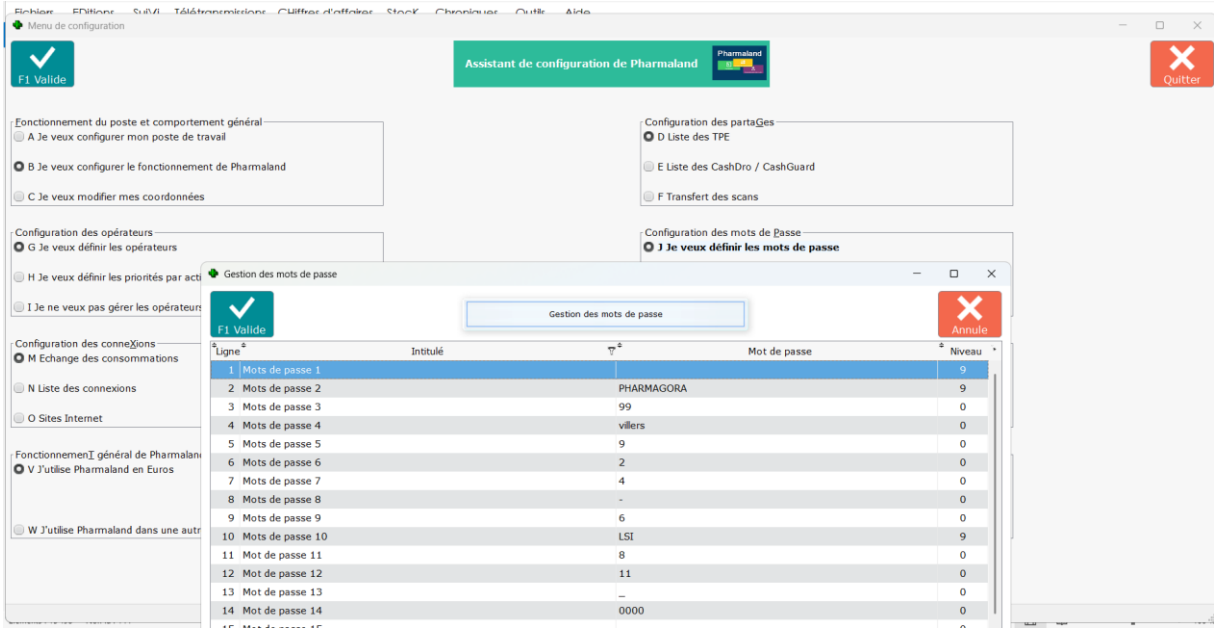
1. Sécurisez vos mots de passe

- Utilisez des mots de passe robustes, personnels et différents pour chaque logiciel ou site web.
- Ne communiquez jamais vos identifiants à une autre personne.
- Ne laissez pas vos mots de passe visibles à proximité des postes informatiques.
- Modifiez immédiatement tout mot de passe suspecté d'avoir été compromis.

Dans Pharmaland : le mot de passe du titulaire permet notamment d'accéder au paramétrage des opérateurs et de leurs habilitations.

Le logiciel permet également de définir différents **niveaux de priorité, de 1 à 9**, afin de contrôler l'accès à certaines fonctions sensibles selon les responsabilités de chaque collaborateur.

Il est donc essentiel de protéger le mot de passe du titulaire et d'attribuer à chacun uniquement les droits nécessaires à son activité.



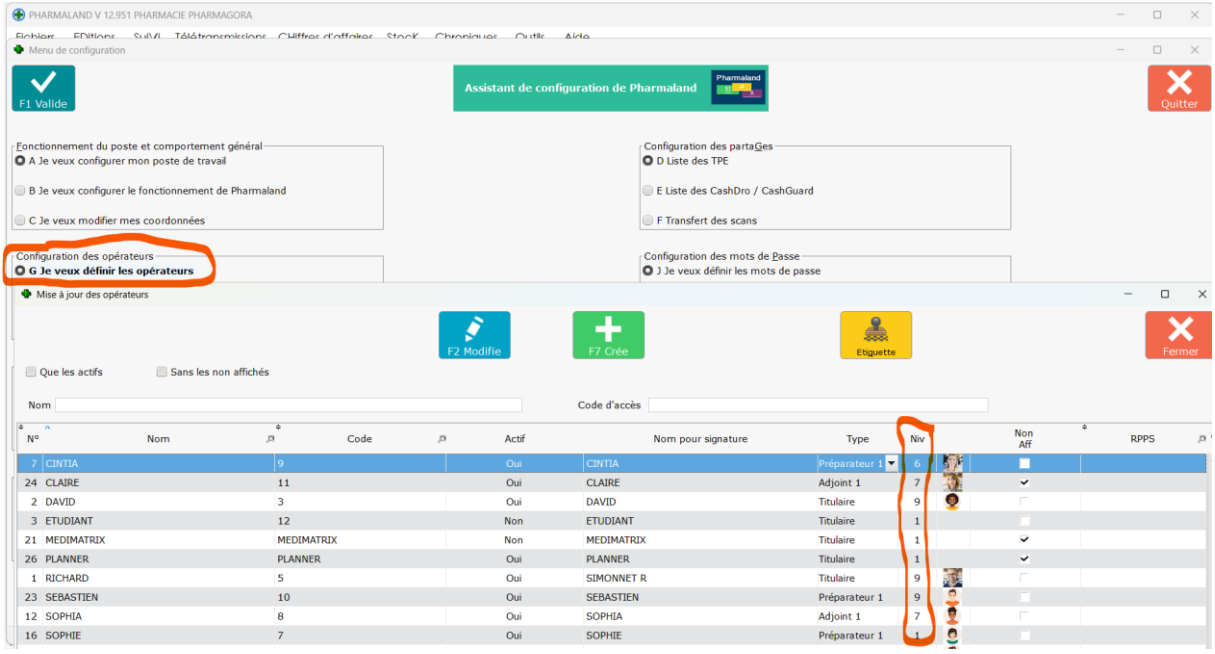
2. Vérifiez les accès de vos collaborateurs dans Pharmaland

- Chaque opérateur doit disposer de son propre code d'accès.
- Vérifiez régulièrement la liste des utilisateurs autorisés.
- Désactivez les comptes des collaborateurs ayant quitté la pharmacie.
- Adaptez les niveaux d'autorisation aux fonctions de chacun.
- Réservez les accès aux paramétrages sensibles aux personnes habilitées.

Pour vérifier les opérateurs :

Avec le mot de passe du titulaire :

Outils → Paramétrages généraux → Assistant de configuration → G – Je veux définir les opérateurs.



3. Contrôlez les logiciels de prise en main à distance

Les logiciels de télémaintenance peuvent représenter un risque lorsqu'ils sont insuffisamment sécurisés.

- Identifiez les logiciels installés : TeamViewer, AnyDesk, Splashtop, RustDesk ou autres.
- Vérifiez que chaque logiciel correspond à un prestataire connu et autorisé.
- Évitez les accès permanents non indispensables.
- N'acceptez jamais une connexion à distance provenant d'un interlocuteur inconnu.

- Ne supprimez pas un logiciel de télémaintenance sans consulter votre support informatique.

4. Surveillez les accès de vos prestataires

Plusieurs intervenants peuvent disposer d'un accès à votre environnement informatique : tiers payant, étiquettes électroniques, téléconsultation, maintenance ou autres services connectés.

- Vérifiez régulièrement les prestataires autorisés.
- Demandez la suppression des accès devenus inutiles.
- Ne communiquez jamais vos identifiants personnels à un prestataire.
- Signalez toute connexion ou intervention inhabituelle.

5. Protégez vos postes informatiques

- Maintenez vos systèmes Windows et logiciels à jour.
- Ne désactivez pas les protections antivirus.
- Évitez l'installation de logiciels non professionnels.
- N'ouvrez pas de pièces jointes ou de liens suspects.
- Verrouillez votre session lorsque vous quittez votre poste.
- Ne branchez pas de clé USB d'origine inconnue ou de téléphone portable pour être rechargé via le poste de travail.

6. Soyez vigilants sur vos sauvegardes

Les sauvegardes sont essentielles pour préserver vos données métier et assurer la continuité de votre activité.

- Respectez les procédures de sauvegarde et de fermeture de Pharmaland.
- Vérifiez que vos sauvegardes sont réalisées régulièrement.
- Signalez toute anomalie à votre support.
- Sauvegarder vos données dans **notre solution Drive Santé HDS**
- Assurez-vous que vos données peuvent être restaurées en cas d'incident.

Une sauvegarde non vérifiée ne garantit pas la récupération de vos données.

7. Réagissez rapidement en cas d'activité suspecte

Certains comportements doivent immédiatement attirer votre attention :

- Une souris qui se déplace seule.
- Des fenêtres qui s'ouvrent sans intervention.
- Une connexion à distance inattendue.
- Des fichiers devenus inaccessibles.
- Un message inhabituel demandant un paiement ou un mot de passe.

En cas de doute, contactez immédiatement votre support informatique Pharmaland. Suivez ses instructions et évitez toute manipulation susceptible d'aggraver l'incident.

Votre sécurité informatique est l'affaire de tous

La **cybersécurité est aujourd'hui un élément essentiel de votre infrastructure informatique** et ne se limite plus à la seule protection de votre logiciel de gestion officinale ou de vos données patients.

Elle concerne **l'ensemble des équipements connectés au réseau de votre pharmacie** : ordinateurs, serveurs, caméras de surveillance, robots de délivrance, étiquettes électroniques, équipements de téléconsultation, sondes de température connectées et bien d'autres dispositifs.

Chacun de ces équipements peut constituer une porte d'entrée potentielle pour une cyberattaque s'il n'est pas correctement sécurisé.

Protéger votre officine, c'est donc sécuriser l'ensemble de votre environnement informatique, maîtriser les accès, maintenir les équipements à jour et garantir la confidentialité de vos données ainsi que la continuité de votre activité.

PHARMALAND — Votre partenaire informatique au quotidien.