Sécuriser et maintenir un portail Portix après audit

Appliquer les contrôles de comptes, fichiers, réseau, sauvegardes et mises à jour depuis les outils de sécurité Portix.

Commencer par les accès

Un audit doit d’abord vérifier les comptes administrateurs, les mots de passe provisoires, la double authentification, les sessions actives et les permissions de chaque rôle.

Contrôler les fichiers

Les zones de téléversement ne doivent jamais exécuter du PHP. Les SVG et les documents actifs nécessitent un filtrage strict, tandis que les archives importées doivent être inspectées avant extraction.

Points de contrôle

- HTTPS imposé et proxies autorisés explicitement ;
- blocage SSRF des adresses privées et locales ;
- filtrage HTML par liste blanche ;
- limitation des connexions et soumissions ;
- journalisation des actions sensibles ;
- sauvegardes protégées et test de restauration ;
- mises à jour signées et vérifiées.

Surveiller sans exposer

Les journaux affichent des adresses masquées et ne doivent pas contenir de mots de passe, de jetons complets ou de clés privées. Les alertes doivent être calculées à partir de l’état réel du serveur.

Préparer la reprise

Avant chaque mise à jour, Portix crée une sauvegarde des fichiers remplacés. En cas d’échec, la restauration automatique ou la page de secours doit permettre de revenir à l’état précédent.

Rythme conseilléContrôler les sessions et alertes régulièrement, puis effectuer un audit complet après chaque changement important de configuration.