Sécurité et maintenance : fiabiliser Portix sans compliquer l’usage

Routes, formulaires, sessions, modules et mises à jour sont contrôlés ensemble afin de réduire les incohérences invisibles dans une simple revue de code.

La sécurité commence par un état cohérent

Un portail peut avoir un bon mot de passe et rester fragile si une route manque dans son manifeste, si un formulaire POST échappe au contrôle CSRF ou si un ancien réglage continue d’activer une fonction que son module a désactivée. Les audits récents de Portix élargissent donc la sécurité au fonctionnement réel du portail.

Tester ce qui s’exécute vraiment

Le contrôle ne se limite plus à lire les fichiers. Les routes GET et POST sont inventoriées, les contrôleurs sont exécutés en HTTP, les formulaires sont rapprochés de leur protection et les espaces authentifiés sont testés avec une session réelle. Cette méthode permet de détecter des défauts qu’un audit purement statique ne voit pas.

Des versions qui se resynchronisent

Lors d’un changement de version, Portix aligne les anciens réglages de services avec le registre actuel des modules. Ce mécanisme évite qu’un menu, une newsletter, un RSS ou une fonction héritée apparaisse encore actif alors que le module correspondant est désactivé. La même logique s’étend maintenant aux contenus officiels, afin que la documentation distribuée corresponde réellement à la version installée.

Des mises à jour qui ne doivent pas toucher aux données client

L’archive d’importation contient uniquement les fichiers applicatifs et métadonnées autorisés. Les comptes, factures, paiements et réglages runtime d’une installation existante restent hors du paquet. Une archive complète de première installation est produite séparément depuis un état nettoyé avec un administrateur initial et un changement de mot de passe obligatoire.

Chaque anomalie importante doit laisser un test

Une correction isolée peut disparaître plusieurs versions plus tard. Portix transforme donc les incidents significatifs en tests de régression : routes de paiement, synchronisation comptable, structure du foyer, cohérence des services et contenu de distribution. Cette discipline est moins spectaculaire qu’une nouvelle fonctionnalité, mais elle améliore directement la fiabilité du logiciel.

Protéger sans rendre le portail inutilisable

Les contrôles techniques doivent rester compatibles avec une navigation simple. Les membres voient les fonctions qui leur sont utiles ; les responsables disposent des opérations correspondant à leur rôle ; les protections serveur restent actives même lorsqu’un bouton est absent de l’interface. La sécurité efficace est celle qui accompagne le fonctionnement normal plutôt que celle qui dépend d’un comportement parfait de l’utilisateur.

La maintenance fait partie de la sécurité

Une version fiable n’est pas seulement une version qui démarre. Elle doit être installable sur une version précédente, préserver les données existantes, produire une sauvegarde et rester cohérente après migration. Les contrôles d’archives, de manifestes et de première installation font donc partie du même niveau d’exigence que la protection des sessions ou des formulaires.