

Plan d'assurance sécurité (PAS)

Le PAS sert à garantir que le produit, le service ou l'infrastructure sera développé, exploité et maintenu dans des conditions de sécurité conformes aux exigences réglementaires, contractuelles et techniques.

1. Organisation et animation de la Sécurité

Chaque Client désigne les Administrateurs de sa plateforme. Ces Administrateurs sont dès lors en contact avec le Support noesya. Ils seront membres des différents canaux de remontées d'information de l'équipe de développement de noesya, et recevrons par ces canaux les informations de sécurité générales. Pour les cas de projets accompagnés spécifiquement, les clients se verront désigner un contact unique qui centralise les informations du projet, que ce soit au niveau fonctionnel ou sécurité : le chef de projet. Ce contact sera le lien privilégié pour traiter les aspects Sécurité spécifiques au projet.

2. Responsabilités de noesya

noesya a la responsabilité durant toute la durée du projet d'assurer la sécurité et la confidentialité des Informations qui sont mises à disposition par ses Clients.

3. Engagement de confidentialité

Les supports informatiques, documents, Informations, données... fournis par le Client restent la propriété du Client. Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel. Conformément à l'article 35 de la Loi Informatique et Libertés, noesya s'engage à prendre toutes précautions utiles afin de préserver la sécurité des Données à caractère personnel et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

noesya s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel : ne prendre aucune copie des documents et supports d'Informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation dans le cadre du projet, sans l'accord du Client ; ne pas utiliser les documents et Informations traités à des fins autres que celles du projet ; ne pas divulguer ces documents ou Informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ; prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du projet ; prendre toutes mesures de sécurité, pour assurer la conservation et l'intégrité des documents et Informations traités pendant la durée du projet ; en fin de projet, procéder à la destruction des Informations du Client et à rendre au Client les Informations lui appartenant.

4. Réversibilité

noesya s'engage à fournir au Client les données gérées par ses plateformes, et à garantir, lors du transfert, la sécurité des données qui lui ont été confiées, conformément à ses obligations. En cas d'arrêt des prestations confiées, l'ensemble des Informations sera restitué. La réversibilité se fait généralement via dump SQL et restitution des medias.

5. Sécurité physique

noesya n'héberge personnellement aucun projet de Client. Les prestations d'hébergement des projets sont sous-traitées. noesya s'assure que les prestataires sélectionnés pour l'hébergement des projets du Client assurent la sécurité physique des systèmes.

noesya s'assure, sauf demande explicite du Client, que l'ensemble des données du projet sont localisées et hébergées en Union Européenne.

Plan d'assurance sécurité (PAS)

6. Sécurité d'exploitation

6.1. Sécurité des réseaux

L'ensemble des sites Internet réalisés pour le Client sont accessibles uniquement en HTTPS.

6.2. Sécurité du développement et de la maintenance

Des sauvegardes multiples et redondantes sont effectuées afin de garantir l'intégrité des informations. Les modifications sont déployées après un processus de validation de tests unitaires. L'ensemble du système est contrôlé par plusieurs outils de monitoring afin de détecter les éventuels problèmes et vulnérabilités, et d'en alerter l'équipe de développement.

6.3. Protection contre les codes malveillants

Quel que soit l'hébergeur utilisé dans le projet les serveurs sont placés sous monitoring constant, et envoient des données de production en temps réel : CPU, Entrées sorties, Mémoire. Tout dépassement de seuils définis engendre l'envoi d'une alerte mail et/ou SMS.

6.4. Sauvegarde

Les codes applicatifs produits par noesya sont stockés sur des forges logicielles (généralement GitHub) et bénéficient des sauvegardes proposées (multiples sauvegardes journalière, redondance, ...). Les bases de données des sites produits sont également sauvegardées (sauvegarde quotidienne, redondance). Ces sauvegardes permettent une remise en place d'une plateforme en cas d'incident de sécurité. Les sauvegardes sont compressées et chiffrées.

6.5. Surveillance

Des traces sur l'ensemble des accès sont sauvegardés sur un an glissant.

6.6. Gestion des certificats

noesya utilise pour la plupart des sites produits des autorités de certification gratuites, comme Let's Encrypt. Cependant le client a la possibilité (et la responsabilité) de fournir à noesya les certificats permettant la mise en œuvre des protocoles sécurisés.

6.7. Contrôle d'accès

Les sites créés par noesya disposent nativement (sauf spécification contraire du Client) d'un système intégré de droits d'utilisateurs, avec à minima 2 rôles distincts, "visiteur" et "administrateur". La quantité de rôles ainsi que les accès auxquels ils donnent droits sont définis en amont du projet avec le Client. noesya propose habituellement des modes d'accès externes s'appuyant sur des fournisseurs d'identités proposant l'un des protocoles suivants : OAuth2 ou SAML2. Cet accès doit être défini en amont du projet et sa mise en place peut faire l'objet d'une facturation complémentaire.

6.8. Audits de sécurité

À la demande du Client, noesya peut faire pratiquer des tests de sécurité sur les sites réalisés. Ces tests sont à la charge du Client. noesya s'engage à fournir son meilleur effort pour corriger les éventuelles failles découvertes par les audits. Selon la complexité de la correction celle-ci peut être soumise à une facturation complémentaire.

6.9. Gestion des incidents liés à la sécurité

noesya s'engage à communiquer sur toute faille qui serait susceptible d'avoir compromis quelque information que ce soit, conformément à sa charte disponible sur le site de gouvernance (<https://gouvernance.noesya.coop/documents/2021/gestion-des-incidents-de-securite-de-l-information>)

7. Révisions

1.0 Date of change: 25/08/2025 - Responsible: Technical team - Summary of Change: Initial

Plan d'assurance sécurité (PAS)

release

noesya-pas-1.0.pdf

25/08/2025

Version 1.0

Page 3

noesya