



Politique de Sécurité

Version 1.0 · En vigueur au 19 juillet 2026

Haadx SAS · Abidjan, Côte d'Ivoire · security@fluwaa.com

Article 1 · Objet et champ d'application

La présente Politique de Sécurité décrit les principes et mesures mis en œuvre par Haadx SAS pour protéger la plateforme Fluwaa (fluwaa.com), les données des Organisations clientes, de leurs membres et des clients finaux qui soumettent des dossiers via les portails publics d'Organisation.

Elle se lit conjointement avec les Conditions Générales d'Utilisation et la Politique de Confidentialité. En cas de contradiction sur un point de protection des données, la Politique de Confidentialité prévaut. La présente politique prévaut sur les aspects strictement techniques et organisationnels de sécurité.

Par principe, la présente politique décrit les mesures de sécurité mises en œuvre au niveau des principes et des garanties apportées à l'utilisateur, sans détailler de configuration technique exploitable. Aucune information contenue dans ce document ne saurait constituer une description exhaustive de l'architecture de sécurité de Fluwaa.

Article 2 · Répartition des responsabilités entre acteurs

La sécurité de la plateforme Fluwaa repose sur une répartition claire des responsabilités entre trois strates d'acteurs :

- Fluwaa (Haadx SAS) · sécurise l'infrastructure, l'application, l'authentification, le stockage et les échanges techniques de la plateforme.
- L'Organisation cliente · demeure responsable de la configuration de son espace, de la gestion de ses membres et de leurs droits d'accès, de la confidentialité de ses identifiants et clés API, ainsi que du contenu et de la légalité des procédures administratives qu'elle traite via Fluwaa.
- Le client final · est responsable de l'exactitude des informations qu'il soumet et de la confidentialité du lien de suivi ou de téléchargement qui lui est communiqué.

Fluwaa n'est pas partie à la procédure administrative traitée par l'Organisation. Elle en fournit l'outil sécurisé, sans se substituer à la responsabilité de l'Organisation quant au contenu, à la légalité ou au résultat de cette procédure.

Article 3 · Authentification et gestion des accès

Fluwaa met en œuvre les mesures suivantes pour protéger l'accès aux comptes :

- Mots de passe et codes PIN hachés selon un algorithme reconnu (Argon2id), jamais stockés en clair.
- Authentification par jeton (access token et refresh token), à durée de vie configurable, complétée d'une double authentification (2FA) par e-mail.
- Activation de compte et de PIN via lien sécurisé à usage unique et à durée de vie limitée (48 heures).
- Révocation immédiate et systématique des sessions actives d'un membre lors de sa désactivation.
- Mécanisme de blocage progressif après plusieurs échecs de connexion consécutifs, avec fenêtre de réinitialisation et durée de blocage configurables, destiné à limiter les attaques par force brute.

Chaque membre d'une Organisation accède uniquement aux fonctionnalités et données correspondant à son rôle (contrôle d'accès basé sur les rôles · RBAC), conformément au principe du moindre privilège.

Article 4 · Protection des données au repos et en transit

- Chiffrement des échanges entre les utilisateurs et la plateforme (HTTPS/TLS).
- Chiffrement au repos des clés de signature électronique propres à chaque Organisation, au moyen d'une clé maître dédiée. Ces clés ne sont jamais stockées en clair.
- Stockage des fichiers (documents, pièces jointes, signatures) intégralement privé. Aucun fichier n'est accessible directement depuis l'extérieur. Tout accès transite par la plateforme, qui délivre des liens sécurisés à durée de vie limitée.
- Identifiants techniques (dossiers, actes, réclamations, sessions de discussion) construits pour ne pas être devinables ou énumérables séquentiellement.

Article 5 · Sécurité applicative et durcissement

- En-têtes de sécurité HTTP conformes aux bonnes pratiques (dont HSTS), politique de partage des ressources (CORS) restreinte à une liste blanche de domaines autorisés.
- Détection et réduction de l'exposition à des dispositifs automatisés malveillants (bots) sur les points d'entrée publics, avec vérification anti-abus (CAPTCHA) disponible sur les formulaires publics les plus sensibles (réclamations, soumission externe de dossier).
- Limitation du nombre de requêtes (rate limiting), proportionnée au plan d'abonnement de l'Organisation et à l'adresse d'origine, sur les points d'entrée publics du portail et de l'API.
- Versions figées des composants d'infrastructure déployés (jamais de version « flottante »), afin de maîtriser précisément les correctifs de sécurité appliqués et d'éviter toute mise à jour non maîtrisée.

Article 6 · Sécurité des API et intégrations

Pour les Organisations activant l'interopérabilité (API publique et webhooks), Fluwaa met en œuvre :

- Authentification par clé API propre à chaque Organisation, stockée sous forme hachée côté Fluwaa.
- Journalisation de chaque appel authentifié à l'API (point de terminaison, statut, horodatage).
- Signature cryptographique (HMAC-SHA256) des webhooks sortants, transmis exclusivement en HTTPS, avec plan de nouvelles tentatives en cas d'échec de livraison.
- Exposition des données par acte configurable au cas par cas par l'Organisation (fonctionnement en liste blanche des champs exposés).

La garde et la confidentialité des clés API et secrets de webhook relèvent de la responsabilité de l'Organisation qui les génère. Fluwaa fournit les mécanismes de hachage et de rotation, mais ne peut être tenue responsable d'une divulgation imputable à l'Organisation elle-même.

Article 7 · Journalisation et traçabilité

Toute action sensible effectuée sur la plateforme (création ou modification d'un acte, traitement d'un dossier, gestion des membres, etc.) fait l'objet d'un enregistrement d'audit, incluant l'auteur, l'adresse IP et l'agent utilisateur associés.

Les modalités de conservation de ces journaux, ainsi que leurs implications au regard du droit à l'effacement, sont détaillées dans la Politique de Confidentialité.

Article 8 · Sauvegardes et continuité d'activité

Fluwaa met en œuvre une politique de sauvegarde régulière de sa base de données, selon une fréquence quotidienne, hebdomadaire et mensuelle, avec des durées de conservation respectivement de 30 jours, 4 semaines et 3 mois. Une procédure de restauration est documentée en interne.

Ces mesures constituent une obligation de moyens. Fluwaa ne garantit pas de taux de disponibilité chiffré, ni de délai de reprise (RTO) ou de perte de données maximale (RPO) déterminés. Un objectif de reprise dans un délai raisonnable est visé en interne, sans constituer un engagement contractuel opposable dans le cadre de la présente politique.

Précision · Les Organisations relevant de la Grille B (contrats publics/entreprise négociés) peuvent convenir d'un niveau de service chiffré (disponibilité, RTO/RPO) dans le cadre de leur contrat particulier. Un tel engagement, s'il existe, prévaut alors sur le présent article pour l'Organisation concernée.

Article 9 · Hébergement et localisation des données

Les données de la plateforme sont hébergées, à la date d'entrée en vigueur de la présente politique, sur un serveur situé en France, chez un prestataire d'hébergement tiers de confiance. Fluwaa a vocation, dans une phase ultérieure de son développement, à proposer un hébergement réparti par zone géographique, avec une affectation automatique par défaut et la possibilité, pour l'Organisation, de choisir la zone d'hébergement de ses données.

Les implications de cet hébergement en matière de transfert de données personnelles sont détaillées dans la Politique de Confidentialité.

Article 10 · Programme de divulgation responsable des vulnérabilités

Toute personne ayant identifié une vulnérabilité de sécurité affectant la plateforme Fluwaa est invitée à la signaler à l'adresse dédiée security@fluwaa.com, plutôt qu'à l'exploiter ou à la divulguer publiquement.

Haadx SAS s'engage à :

- accuser réception de tout signalement dans un délai de 72 heures ouvrées ;
- traiter chaque signalement de bonne foi et y apporter un correctif dans un délai proportionné à sa gravité ;
- ne pas engager de poursuites à l'encontre d'un chercheur agissant de bonne foi, dans la limite d'un cadre raisonnable · absence de divulgation publique avant correctif, absence d'exploitation au-delà de la démonstration de la faille, absence d'accès ou d'atteinte aux données réelles d'une Organisation ou d'un client final.

Article 11 · Conformité et cadre réglementaire

Fluwaa met en œuvre les mesures de sécurité décrites dans la présente politique dans une logique de conformité aux bonnes pratiques reconnues (référentiel OWASP notamment), à la loi ivoirienne relative à la protection des données à caractère personnel (loi n° 2013-450) et, pour les Organisations et clients finaux résidant dans l'Union Européenne, au Règlement Général sur la Protection des Données (RGPD).

Les rôles respectifs de responsable de traitement et de sous-traitant entre Fluwaa et l'Organisation sont précisés dans la Politique de Confidentialité.

Article 12 · Signature électronique et vérification des documents

Les documents signés électroniquement via Fluwaa font l'objet d'une empreinte cryptographique (hash SHA-256), d'un horodatage et d'un code de vérification publique consultable à l'adresse o.fluwaa.com/verify/{identifiant}.

Cette vérification atteste l'intégrité technique du document et son origine. Elle ne constitue pas une appréciation de la validité juridique du contenu du document, ni une qualification du niveau de signature électronique au sens d'un texte particulier. Il appartient à l'Organisation de s'assurer de la portée juridique de sa signature dans le contexte d'usage visé; celle-ci relève, en tout état de cause, de l'appréciation des autorités compétentes et de la loi applicable.

Article 13 · Mise à jour de la présente politique

Haadx SAS peut faire évoluer la présente Politique de Sécurité à tout moment, notamment pour refléter l'évolution de l'infrastructure ou des mesures de protection mises en œuvre. Toute modification substantielle sera notifiée aux Organisations selon les modalités prévues par les Conditions Générales d'Utilisation.

Article 14 · Contact

- E-mail sécurité · security@fluwaa.com
- E-mail support · support@fluwaa.com
- Adresse · Haadx SAS, Abidjan, Côte d'Ivoire

Date d'entrée en vigueur : 19 juillet 2026